**Ideation Phase**

**Define the Problem Statements**

|  |  |  |  |
| --- | --- | --- | --- |
| **DATE** | | **24 September 2022** | |
| **TEAM ID** | | **PNT2022TMID49682** | |
| **PROJECT NAME** | | **Web Phishing Detection Using Machine Learning** | |
| **MAXIMUM MARKS** | | 2 | |
| **S.NO** | **PARAMETER** | | **DESCRIPTION** | |
| 1. | Problem Statement | | Phishing detection techniques do suffer low detection accuracy and high false alarm especially when novel phishing approaches are introduced. Besides, the most common technique used, blacklist-based method is inefficient in responding to emanating [phishing attacks](https://www.sciencedirect.com/topics/computer-science/phishing-attack) since registering new domain has become easier, no comprehensive blacklist can ensure a perfect up-to-date database. Furthermore, page content inspection has been used by some strategies to overcome the false negative problems and complement the vulnerabilities of the stale lists. Moreover, page content inspection algorithms each have different approach to [phishing website detection](https://www.sciencedirect.com/topics/computer-science/website-phishing-detection) with varying degrees of accuracy. | |
| 2. | Idea | | * Web Phishing Detection  1. **Identify the criteria** that can recognize fake URLs 2. **Build a decision tree** that can iterate through the criteria 3. **Train our model** to recognize fake vs real URLs 4. **Evaluate our model** to see how it performs 5. **Check for false positives/negatives**  * **Increase user alertness to phishing risksAssess the impacts of cyber security awareness training Segment phishing simulationTrain our model to recognize fake vs real URLs Change behavior to eliminate the automatic trust response**Identify the criteria that can recognize fake URLs.Build a decision tree that can iterate through the criteria**Install a cyber security culture and create cyber security heroes.** * Install a cyber security culture and create cyber security heroes Evaluate our model to see how it performs Assess the impacts of cyber security awareness trainingstrong password policies and reminding employees about the risks that can come in the format of attachments, emails and URLsProvide ongoing communication and campaigns about cyber security and phishing.This is best done by designing rigorous user education programs that help users not only identify fraudulent emails but also provide specific guidance on how to handle suspect communicationsAlarming content full of warnings and potential consequencesIn the sections below, we focus on safely handling emails that do manage to breach the security of the software layerantivirus software;both desktop and network firewalls; antispyware software; antiphishing toolbar (installed in web browsers);. Ensure that all applications, operating systems, network tools, and internal software are up-to-date and secure. Install malware protection and anti-spam software Eliminate the cyber threat risk level**.** | |
| 3. | Novelty | | * Future Work will include using another algorithm like deep-learning for phishing web page detection and compare the effectiveness with the current result.More also, a web browser plug -in will be developed based on an efficient algorithm to detect phishing website and thus protect users in real time. | |
| 4. | Social impact | | * Phishing has a list of negative effects on a business, including loss of money, loss of intellectual property, damage to reputation,and disruption of operational activities.These effects work together to cause loss company value,sometime with irreparable repercussions. | |
| 5. | Business Model | | * Phishing is big business.Attacks have shown record growth in recent years, and a solid security awareness program is an integral part of any defense-in-depth strategy. Sophos Phish threat educates and tests your end users through automated attack simulations,Quality security awareness training, and actionable reporting metrics.Phish Threat provides you with the flexibility and customization that your organization needs to facilitate a positive security awareness culture. | |
| 6. | Scalability of solution | | * Use Web-Phishing Protection and web-spam software to protect yourself when malicious message slip through to your computer.Web-Malware software is programmed by security researches to spot even the stealthiest malware. * Certain Web-Phishing solutions Scan the content of inbound and internal emails for any sign of language that suggest a potential phishing or impresonation attack. Other Web-Phishing technology scans the links and attachments in email and blocks users from accessing them if they are determined to be suspicious. * E-Banking Phishing Website can be detected based on some important characteristics like URL and domain identity and security and encryption criteria in the final phishing detection rate once a user makes a transaction online when he makes payment through an e-banking website our system will use a data mining algorithm to detect whether the e-banking Website is a phishing website or not. | |