Project Design Phase-I
Proposed Solution Template

Date	02 Oct 2022
Team ID	PNT2022TMID23940
Project Name	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)	Most phishing attacks exhibit the application of social engineering tactics. Social engineering is the most significant factor that leads to malicious hacking crimes since 99% of cyber-attacks need some level of human intervention to execute. However, many phishing campaigns are made to look legitimate, but these interactions enable macros and malicious code to run. Whereas it may be easy to blame the system users, it is also important to note that phishing has become increasingly sophisticated. It is increasingly becoming challenging to note new attacks since the perpetrators make the email look as coming from a trusted source. However, social engineering is playing a central role in facilitating these crimes since
2.	Idea / Solution description	Defender's anti-phishing solution uses machine learning modules to check inbound messages for key indicators that they may be a phishing attempt. These include the header, sender's address and message content. When a threat is detected, the attack is blocked. Defender also has the capability to detect and block malicious links and attachments.
3.	Novelty / Uniqueness	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 since registering new domain has become easier, no comprehensive blacklist can ensure a perfect up-to-date database.
4.	Social Impact / Customer Satisfaction	Millions of people are being affected and billions of dollars are getting stolen. Phishing is a technique used to extract

		personal information from victims by means of deceptive and fraudulent emails for identity theft. As a result of this, the organizations as well consumers are facing enormous social effects.
5.	Business Model (Revenue Model)	Making subscription in URL phishing detection and payable installation of software (anti-phishing)
6.	Scalability of the Solution	The main ideas are to move the protection from end users towards the network provider and to employ the novel bad neigh- boohood concept, in order to detect and isolate both phishing e-mail senders and phishing web servers.