Project Design Phase – I

Date	24-09-2022
Team ID	**PNT2022TMID33764**
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution

S.No.	Parameter	Description
1.	*Problem Statement (Problem to be solved)*	The problem with phishing is that a holistic solution that works to protect users securely from being phished does not exist. As the defences against phishing have evolved, so have the current phishing methods. As a result, the need for more advanced methods of security to identify phishing is important.
2.	*Idea / Solution description*	Our proposal is to develop self-management architecture for phishing detection and isolation. This architecture includes several elements, namely: e-mail servers, network routers, network firewalls, telescopes, phishing e-mail senders, phishing web servers, and a phishing detector. The idea is to analyze the data using self-learning techniques and the bad neighbourhood concept. This will result into two different lists. The first one contains IP addresses that distribute phishing messages While the second contains names and IP addresses of phishing web servers.
3.	*Novelty / Uniqueness*	Instead of relying on end users, we propose to move protection towards the ISP, who should block malicious servers and, in this way, offer transparent protection for all end users.
4.	*Social Impact / Customer Satisfaction*	Beyond monetary damages, businesses that are breached lose public trust and must work to secure their databases. It is in the best interest of the business to ensure customer satisfaction and build customer loyalty.
5.	*Business Model (Revenue Model)*	The high number of phishing attempts makes it impossible to manually cope with such attempts. Therefore demand for Complete automation of detection and isolation in fast and reliable way grows. The idea is to develop and market (in collaboration with ISP) an integrated architecture that is able to detect and block phishing. ISPs could offer this as a service.
6.	*Scalability of the Solution*	To ensure scalability, we propose the use of flow analysis instead of deep packet inspection. Moreover, with flow based approaches it is possible to analyze flow patterns and compare the network behaviour of multiple sources.