INFORMATION SECURITY MANAGEMENT

REVIEW - 1

TOPIC NAME

PHISHING DETECTION USING MACHINE LEARNING (Chrome Extension)

TEAM MEMBERS

AMAN KUMAR SINGH 19BCE2589

MOGALAPU JAYA SRIKAR 20BCE2041

ABSTRACT

The goal of our project is to develop a solution for detecting phishing and dangerous web links using machine learning. Our work will lead to the creation of software that uses a machine learning algorithm, to detect fraudulent URLs.
Phishing is a method for getting access to user passwords and sensitive information by pretending to be a reliable website. In phishing, a fake website that seems exactly like the real one but contains malicious code that collects and sends the user's login information to the phishers.

Customers of banking and financial services may suffer significant financial losses as a result of phishing attempts. To detect the presence of harmful programmes, the typical method to phishing detection has been to either employ a blacklist of known phishing URLs or heuristically evaluate the properties of a suspected phishing page. The heuristic algorithm uses trial and error to determine the threshold for classifying harmful and benign links. The disadvantages of this method include its lack of accuracy and flexibility to new

phishing links. By building different categorization algorithms and comparing their performance on our dataset, we hope to apply machine learning to solve these disadvantages. On a dataset of phishing URLs from the UCI Machine Learning repository, we will evaluate methods such as Logistic Regression, SVM, Decision Trees, and Neural Networks, and choose the best model to construct a browser plugin that may be distributed as a chrome extension.

THANK YOU