ABSTRACT

This project aims to use an intelligent, versatile, and reliable method to recognise and classify e-banking and other phishing websites. In this project, we check if a given URL is Phishy ornot by looking it up in a dataset, and if it's not there, we'll break it down based on factors like the URL, Domain Identity and Security, and encryption requirements, and determine whether it's Phishy or not. Phishing websites are those that ask users for personal information for a malicious reason.

Phishing is described as the art of emulating a website of a creditable firm intending to grab user's private information such as usernames, passwords and social security number. Phishing websites comprise a variety of cues within its content-parts as well as browser-based security indicators. Several solutions have been proposed to tackle phishing. Nevertheless, there is no single magic bullet that can solve this threat radically. One of the promising techniques that can be used in predicting phishing attacks is based on data mining. Particularly the "induction of classification rules", since anti-phishing solutions aim to predict the website type accurately and these exactly fit the classification data mining. In this paper, we shed light on the important features that distinguish phishing websites from legitimate ones and assess how rule-based classification data mining techniques are applicable in predicting phishing websites

Keywords: *Phishing websites, URL, Domain, usernames, passwords*