**ABSTRACT**

A phishing technique was described in detail in a paper and presentation delivered to the 1987 International HP Users Group. Ever since the concept of phishing has been introduced it’s growing so fast. The problem is we do not have enough resources to detect any phishing website in real time. Phishing attempts have grown 65% in the last year and it’s still growing so fast because the average cost of a phishing attack for mid-size companies $1.6 million. The technique for detection for phishing website has been proposed and project has been implemented in this called ‘PHISHING DETECTION THROUGH MACHINE LEARNING’. In this project I have emphasized on the method of detection through the URL also called ‘DECEPTIVE PHISHING’, because it is the most common way people visit the websites and links. The project uses the idea of Neural Network and the model has been trained for the detection of fake website. Some machine learning algorithms have been used to check the best result. The result shows that suing the random forest algorithm is the best fit for the model having 97% of accuracy. The main aim for this project is to detect the malicious website and detect the location of the server. On top of that twenty different techniques have been used to analyze the URL type which decides if the URL is phishing or not. In the second part of the project another type of phishing has been introduced. It is called ‘SPEAR PHISHING’; in this technique I have used the email header to detect the email path and some security protocols to make sure that the email we get is safe or not. In the third section I have noted some common type of phishing through Wikipedia. It is very useful for the people who do not have any prior knowledge in this area. So, it is helpful for those people to have some basic idea of phishing and its type along with how to get rid of it using this website.