**Abstract**

Communication by email is one of the most popular and commonly used by people today. Emails can be utilized in various forms and because of the versatility of email communication, sensitive and confidential information can be distributed through emails. Phishing is a method of obtaining this sensitive/confidential information from emails by tricking people into revealing this information. Phishing is a social engineering technique that is deployed to obtain sensitive/confidential information from victims by tricking the victim into believing that malicious host is a reputable host. Phishing attacks have characteristics that allow for easier distinguishing between safe emails and malicious emails since attackers cannot take the identity of the reputable source and they all have a certain goal when employing their attacks. For this research, the main approach of detecting these phishing emails was through classification and extracting features from the emails themselves to create the dataset. Then, machine learning algorithms would use the dataset to make predictions on whether an email was safe (ham) or phishing. Highest results for the algorithms currently marks at 93.50%

**Introduction**

**Related Work**

**Proposed System**

**Features**

**Results**