**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**

* Introduce the topic of phishing
  + What it means and why is this type of attack employed
  + The different types of phishing
    - i.e spearing, whaling, etc.
* Report the losses of phishing attacks of victims and who was targeted
* Introduce the methodology that will be used to detect the phishing emails
  + Pre-processing: Python NLP
    - Explain what pre-processing is
  + Machine Learning: various algorithms
    - Explain what machine learning is

**Related Work**

* Explain how a lot of research has been done on phishing websites but far less on phishing emails specifically
  + Explain their approach to performing the analysis on phishing websites
* Explain how the research that has been performed on phishing emails differs from the research that I intend to perform
  + My method of preprocessing will place more emphasis in the amount that focuses on NLP than other research performed in the field

**Proposed System**

* Explain the how the data comes from being in raw emails to a dataset
  + Explain why certain choices were made
    - i.e focus on speed over accuracy or why more words were chosen
* Create a visual that explains the process simpler:
  + Emails -> Email Classification -> NLP analysis -> Feature Extraction -> Dataset creation -> Results and Machine Learning Analysis

**Features**

* Words
  + Explain which words were chosen and why they were chosen
    - Checked the frequency of which keywords show in phishing emails
  + Explain how the NLP analysis helped this analysis
    - Explain the process of stemming
* Part-of-speech Analysis
  + Explain what POS analysis and how it was performed
  + Explain why it was performed
    - The objective of phishing emails is to cause action thus action verbs are important

**Classifiers**

* Explain what each classifier that was used in machine learning analysis
* Explain if different types of models were used for the same classifier, then why

**Dataset**

* List the total number of features of the dataset
* List the total number of phishing emails
* List the total number of ham emails
* List the total number of emails

**Results**

* Explain what k-cross fold validation is
* Explain what classifies as a false positive result
* Explain what classifies as a false negative result
* Explain what classifies as correctly classified result (ham and phish)
* Explain results of each classifier & display them

**Conclusion**

* Summarize all that was done to get features
* Summarize results of all findings
* Talk about what these mean as a result
* Where room for improvement lies