|  |  |  |  |
| --- | --- | --- | --- |
| Abstraction | Review Date | Publish Date | Title |
| Discusses a simple way to implement the sentiment analysis using ML. | 2019 | 10-Apr-2020 | social engineering attack detection in  online environments using machine learning  - Spring |
| This paper discusses how to detect Social Engineering Attacks using Supervised machine learning | - | 30-Aug-2018 | Towards an Automated Recognition System for Chat-based  Social Engineering Attacks in Enterprise Environments - ACM |
| This paper focuses on how to detect Social Engineering attacks by building a Finite State as a direction to warn the end user. | - | 2-June-2018 | FINITE STATE MACHINE FOR THE SOCIAL ENGINEERING  ATTACK DETECTION MODEL: SEADM |
| This paper describes the modern ways of SE attacks and how to deal with them. | - | 24-Oct-2014 | Advanced social engineering attacks |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Accuracy | Datasets | Algorithms |
| 92% | [SEADer](https://github.com/npolatidis/seader) | Naïve bayes  Gaussian Law  Fuzzy logic  Decision Trees  Neural Networks |
| 88.9% | - | Naïve bayes  Support Vector Machine |

|  |  |  |  |
| --- | --- | --- | --- |
| Abstraction | Review Date | Publish Date | Title |
| Performing multiple steps with scores to classify the database, including intent/spelling/link-detection techniques. | August 2019 | August 2019 | **SEADer: A Social Engineering Attack Detection method based on Natural Language Processing and Artificial Neural Networks** |
| Uses natural language processing techniques to  detect questions and commands.  Each extracted topic is compared against a topic blacklist | 2016 | 2016 | **Detection of Social Engineering Attacks Through Natural Language Processing of Conversations** |
| Processing text in conversation into a network of steps, each step has its own model for detection a feature about text to determine if it’s malicious or not. | 2018 | 2018 | **Catch me, Yes we can! - Pwning Social Engineers using Natural Language Processing Techniques in Real-Time** |
| Using Logistic Regression to classify the URL . | 2020 | 2020 | **AN AUTOMATED SYSTEM FOR DETECTION OF SOCIAL ENGINEERING PHISHING ATTACKS USING MACHINE LEARNING** |
| Classifying data in text conversations into normal or abnormal, depending on J48 decision tree. | 2020 | 2020 | **An Analysis of Various Social Engineering Attack in Social Network using Machine Learning Algorithm** |

|  |  |  |
| --- | --- | --- |
| Accuracy | Datasets | Algorithms |
| Precision 100%  Recall 60% | \_ | Hobbs Algorithm |
| \_ | \_ | SEADM |
| \_ | \_ | SEADM |
| \_ | \_ | SEADM, SEADMv2 |
| Precision 100%  Recall 88.9% |  | Text scanning.  MatchTopic Algorithm. |

s

|  |  |  |  |
| --- | --- | --- | --- |
| Abstraction | Review Date | Publish Date | Title |
| we have developed a method that detects social  engineering attacks that are based on natural language processing  and artificial neural networks. This method can be applied in  offline texts or online environments and flag a conversation as a  social engineering attack or not. | **22 March 2020** | **23 December 2019** | **social engineering attack detection in online**  **environments using machine learning** |
| using deep learning, it was checked whether the web sites are real or not by using neural networks and support vector machine, decision tree and stacked autoencoders as classification methods. As a result of the study, 86% success rate was reached by using stacked autoencoders which are a part of deep learning techniques. |  | **06 July 2018** | **Phishing Analysis of Websites Using Classification Techniques**  **“Book”** |
| In this paper, a  phishing detection system which can detect this type of attacks by using some  machine learning algorithms and detecting some visual similarities with the help  of some natural language processing techniques. Many tests have been applied on  the proposed system and experimental results showed that Random Forest algorithm  has a very good performance with a success rate of 97.2%. |  | **March 2018** | **NLP Based Phishing Attack**  **Detection from URLs** |
|  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Accuracy | Datasets | Algorithms |
| * Decision Tree results for the standard dataset = 73% * Decision tree results for the compound dataset = 90% | **Bezuidenhout**  **et al. (2010)** | * **Rosenblatt’s perceptron rule** * **Gaussian Naïve Bayes** * **Decision Tree classifier** * **Random Forest classifier** |
| * Results of neural network = 79% * Results of deep learning = 84% | * **Google’s secure browsing API** * **PhishTank website** | * **feedforward neural network.** * **Stacked Autoencoders** |
| * 97.2% success rate | * **PhishTank** * **Yandex Search API** | * **Random Forest** |
|  |  |  |