Computer Science and Information Technologies
Vol. 1, No. 1, May 2020, pp. 1~12
ISSN: 2722-3221, DOI: 10.11591/csit.v1i1.p1-12

Email phishing: Text classification using natural language processing

Priyanka Verma, Anjali Goyal and Yogita Gigras
The Northcap University, Gurgaon, Haryana, India

Article Info

Article history:

Received Apr 14, 2019
Revised Nov 12, 2019
Accepted Jan 7, 2020

Keywords:

Classification report
Confusion metrics
Email phishing
Machine learning
Natural language processing
Social engineering

ABSTRACT

Phishing is networked theft in which the main motive of phishers is to steal any person's private information, its financial details like account number, credit card details, login information, payment mode information by creating and developing a fake page or a fake web site, which look completely authentic and genuine. Nowadays email phishing has become a big threat to all, and is increasing day by day. Moreover, detection of phishing emails has been considered an important research issue as phishing emails have been increasing day by day. Various techniques have been introduced and applied to deal with such a big issue. The major objective of this research paper is giving a detailed description on the classification of phishing emails using the natural language processing concepts. NLP (natural language processing) concepts have been applied for the classification of emails, along with that accuracy rate of various classifiers have been calculated. The paper is presented in four sections. An introduction about phishing its types, its history, statistics, life cycle, motivation for phishers and working of email phishing have been discussed in the first section. The second section covers various technologies of phishing- email phishing and also description of evaluation metrics. An overview of the various proposed solutions and work done by researchers in this field in form of literature review has been presented in the third section. The solution approach and the obtained results have been defined in the fourth section giving a detailed description about NLP concepts and working procedure.

Corresponding Author:

Priyanka Verma,
The Northcap University,
India.
Email: priyanka17csp008@ncuindia.edu

1. INTRODUCTION

Phishing is basically a networked theft in which the main motive of phishers is to steal any person's private information, its financial details like account number, credit card details, login information, payment mode info and many more. Phishing is a technique in which an attacker creates and develop a fake page or a fake web site, which look completely authentic and genuine, but it is not. The attacker deploys the same and make people to enter their credentials. Nowadays this is done mainly through e-mails. Many fake sites are available and are used by phishers to fraud people by sending fake mails and steal their private info or make them a victim of email phishing by sending any kind of malicious link or pop-up in mails that the user will unknowingly open and thus got stuck in their trap. It is a form of fraud in which the attacker represents himself to be genuine entity and attack via communication channels. Phishing is broadly classified in three categories. Spear phishing**:** Targeting a single or an individual or the crowd of people having common interest, termed as spear phishing. In this type of phishing the major target of the phisher is stealing and using

the private details about the target to assure their chances of success. Clone phishing: in this type of phishing attack, the attacker creates a clone of existing email and attach malicious content or link with the mail in order to steal person's info or any fraud. The email with malicious content is then sent from a spoofed email address that appears to be an original email address. It may claim to be a resend of the original or an updated version to the original. It is not target specific. Any kind of person can come and enter their credentials. They just need to collect the credentials of the crowd for their own purpose. Whaling: This type of phishing attack has been invented from spear phishing attacks which are directed mainly at senior executives or other high-level targets. In this attack, the malicious content to target an upper level person like the CEO or the person's role in the company is created.

2. BACKGROUND

This section gives a description on the history and statistics, life cycle, motivation for phishers, email phishing and its working.

2.1. History

The term "phishing" was invented in early 1990s, when a huge number of users with fake credit card details, generated an algorithm for stealing user's information. These people registered themselves on AOL (America online) website without any confirmation and started using AOL's system resources. By 1995, AOL was able to stop the random credit card generators, but the warez group moved on to other methods, specifically pretending to be AOL employees and messaging people via AOL Messenger for their information [1]. This quickly became such a problem that on January 2, 1996, the word "phishing" was first posted in a Usenet group dedicated to American Online [1]. Phishing celebrated its 21th birthday last year. This practice got its start on AOL when a group of hackers created a tool, which generate random credit card numbers that were used to create AOL accounts. They tricked users for stealing their private information like SS numbers, credit/debit card numbers, DOB, credentials etc. They would then deploy other AOL accounts whom they can use further to do phishing attacks. Since people become aware about this scam so, phishers then found out new way of phishing and chooses email communications that were very cheap, easy and very hard to get caught.

A comparative analysis of phishing attacks in year 2016-2018 there is a huge amount of increase in attacks, and changes of these attacks to grow more in coming years because if lack of awareness shown in Figure 1. As per Symantec's 2018 Internet Security Threat Report (ISTR) [3], a whopping 54.6% of all email is spam. Their data shows that an average user receives about 16 malicious mails per month that is a very huge amount. 92.4% malware is delivered via mail. So, it is a big threat and employee has to be trained to keep aware. It is not even possible for every employee to identify every malicious email. So, it is necessary to have right security solutions.

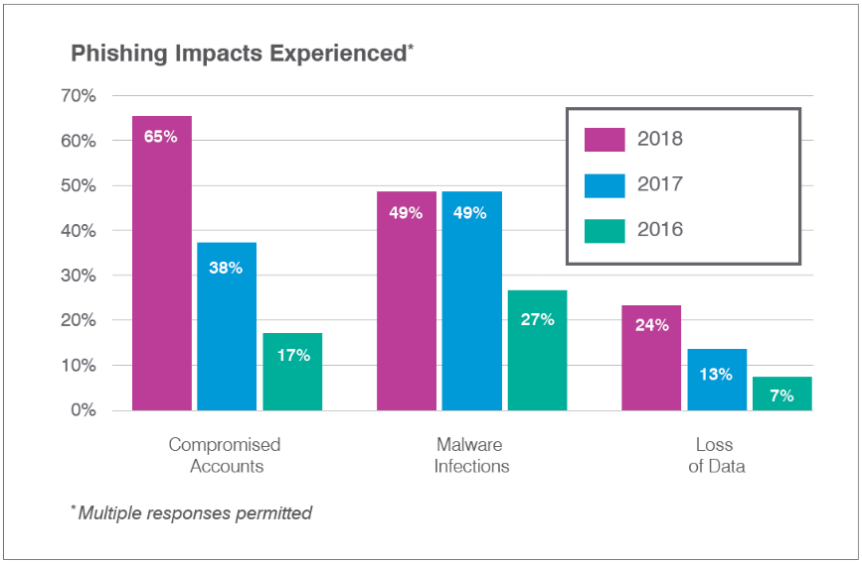

Figure 1. Phishing attacks experienced in last three years [2].

2.2. Life cycle

Figure 2 shows the life cycle of phishing. From beginning to end, the phishing process involves following steps:

Stage 1: Plan and setup creating: It is the very first step of phishing, in which the attackers identify the targeted organization or individual. Their aim is to gather information about the targeted organization and its network. This can be done by visiting that place or by monitoring the traffic going in and out of that organization's network. The next step is to create setup for the attacks by possible means like creating fake websites and sending emails with malicious links and content, which will then redirect the users towards some fraud web page.

Stage 2: Sending malicious content: The next step in phishing cycle is to send the spoofed emails, e.g., impersonated as some genuine organization's email to the victim using the collected email addresses, and asking the user to update their sensitive or personal information urgently by clicking on some malicious link.

Stage 3: Invading/breaking-in: Once the victim clicks the fraud link, either a malware is installed on the system or the user may be redirected to some fake malicious page which makes the attacker to gain access to the system or change the system configuration to maintain that access.

Stage 4: Extracting useful data: After gaining control to the victim's system, the required data are extracted, and if any how the user unknowingly gives his/her account details to the attacker, that may result in huge financial losses to the user. In case of exploitation attacks, the attacker can also perform DDOs [4] attack to damage the user's system or can get the system's remote access and the data he wants.

Stage 5: Escaping/Breaking-out: This is the main step for phishers, as it involves clearing of tracks and evidences. After extracting all the juicy information, the attacker eliminate the evidences like the fake websites and accounts. The attackers can also keep a track of the victim for future attacks.

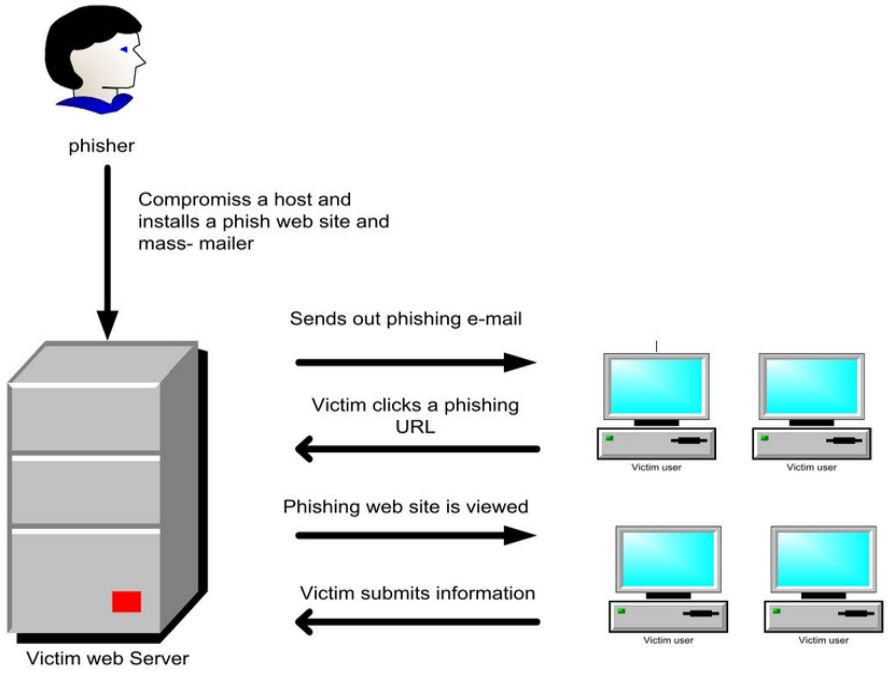

Figure 2. Life cycle of phishing [5]

2.3. Motivation for phishers

Phishers take advantage of the lack of awareness and ignorance of the users and for stealing their information. Nowadays phishers are very much capable in finding out loopholes in the newly generated technique to commit successful attacks. There are various factors other than financial gains that encourages attackers to commit the crime. Some of the factors are as follows:

– Stealing login information/credentials: Phishers managed to steal the login credentials of various online services like banking applications, amazon, G-mail, Facebook, eBay etc. from the user by means of fake emails or warning messages for updating passwords and information.

- Stealing banking details/credentials: Various personal information like A/c number, credit/debit card details, CCV number, and login credentials of banking applications etc. serves as a good bait for the phishers.
- Capturing private information: Private data, such as Aadhar number, residential address, contact details, telephone number, can act as a huge demand for many organizations and marketing companies.
- Stealing of confidential documents and trading secrets: As per nature of spear phishing in targeting big organizations, organization secrets and documents can pay a very good price to phishers from opposition and attentive parties.
- Recognition and opprobrium: A cognitive aspect about phishing that's very interesting, in which information is stolen not for stealing purpose but mainly for gaining recognition and bad fame among their friends/peers.
- Exploitation of security loop holes: Inquisitive nature of people especially hackers, have a fad in their nature for finding out robustness of system that they even write code for exploiting the system and try it out on someone else's system to launch phishing attack or even sell the system to other phishers.

2.4. Email phishing

Email phishing is the act of tricking the mail recipient business or any other entity in order to obtain sensitive personal information by sending fake mails and making the receiver believe that it came from a genuine source. Data extracted after phishing is often used to do identity theft or to steal login details to have access to online accounts. Spoofing is a way similar to email phishing that it uses techniques to make people ensure that the mails have come from a legitimate source that they can trust and thus become victim of fraud. It uses the email header to make it looks like an original source. Similarly, spoofed IP's use forged IP address to fool the user's computer and making them believe that it came from a trusted source. Various sites can be used to create and send fake mails: https://emkei.cz/, https://getgophish.com/, www.temp-mail.org. Figure 3 showing fake email message in name of amazon enterprise.

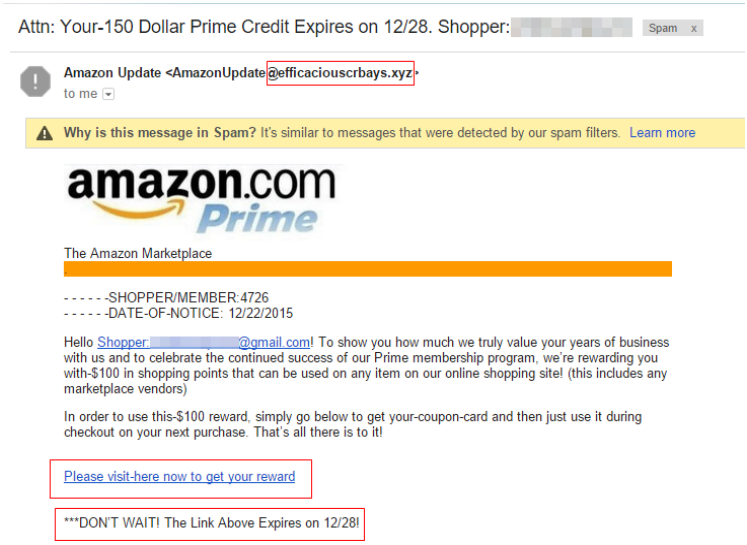

Figure 3. Showing fake email message in name of amazon enterprise. [6]

2.5. Working of email phishing

The working of email phishing as shown in Figure 4 mainly incudes seven steps:

1. Compromise web server: the very first step of attacker is to break into the web server. This can be done using various attacks and tools like DDOS attack and available phishing tools.
2. Sending phishing e-mails: the attacker then sends the mail containing malicious link or content or even fake mails asking for private information to the victim/receiver.
3. Received mail: the user/victim who is unaware of the fact that the mail is not a genuine one, clicks on the link provided in the mail.
4. Access website: after clicking on the link the user is directed towards the compromised website.

5. Phishing website appears: the attacker then sends the fake and malicious site to the user end asking for information.
6. Submit information: the user being unaware about the fact that the site is not a genuine one enters his/her asked information and become a victim of mail phishing.
7. Make use of information: after getting juicy information from the user, the attacker then takes advantage of that information or may misuse that or even blackmail user.

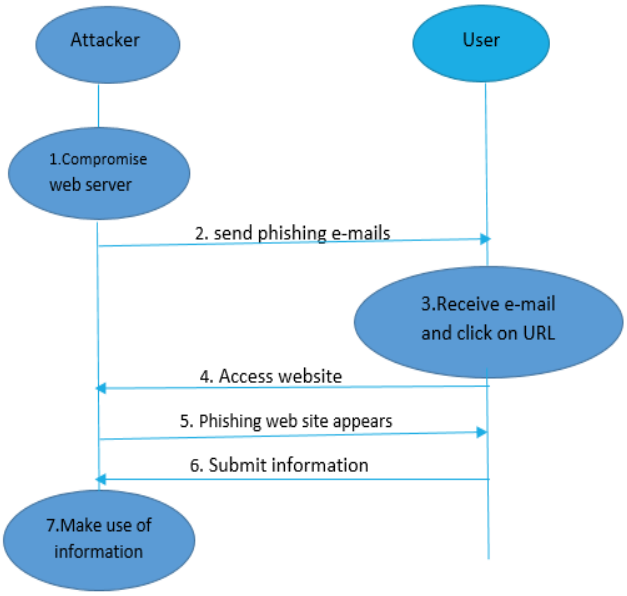

Figure 4. Procedure of email phishing

3. EVALUATION METRICES

Many researchers use evaluation metrics for the evaluation and experimentation of their research techniques [7]. The main objective of evaluation metrics is to state phishing mails from a set of given malicious and genuine mails. Given below the various evaluation metrics:

True positive rate (TPR): It states the ratio of phishing mails detected with respect to all malicious and genuine mails.

$$TPR = \frac{n_{phishing \rightarrow phishing}}{n_{phishing \rightarrow phishing} + n_{phishing \rightarrow ham}} = \frac{TP}{TP + FN}$$

False positive rate (FPR): It states the ratio of genuine mails that were improperly detected as phishing mails.

$$FPR = \frac{n_{ham \rightarrow phishing}}{n_{ham \rightarrow ham} + n_{ham \rightarrow phishing}} = \frac{FP}{TN + FP}$$

Accuracy (A): It measures the rate of mails detected correctly as phishing with respect to all detected phishing mails.

$$A = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP}+\mathrm{FP}+\mathrm{FN}+TN}$$

4. TAXONOMY OF PHISHING ATTACKS

Phishing attacks can be determined as per multiple techniques used by the phishers to steal personal information of victim. Phisher can fraud a victim either by sending malicious link via email or by creating fake website to trap the users and stealing their personal information. Email threats have become a persistent source of cyber security practitioner anguish. However, lack of knowledge and understanding among the users acts as a benefit for the phishers for performing phishing attack for stealing their credentials. An attacker can fraud any innocent user either by sending spoofed emails or by using fake websites.

Various techniques like social engineering, subterfuge, wireless medium, malicious code, key loggers, and screen capture can also use to steal personal information. The categorization of Phishing attacks is shown in Figure 5.

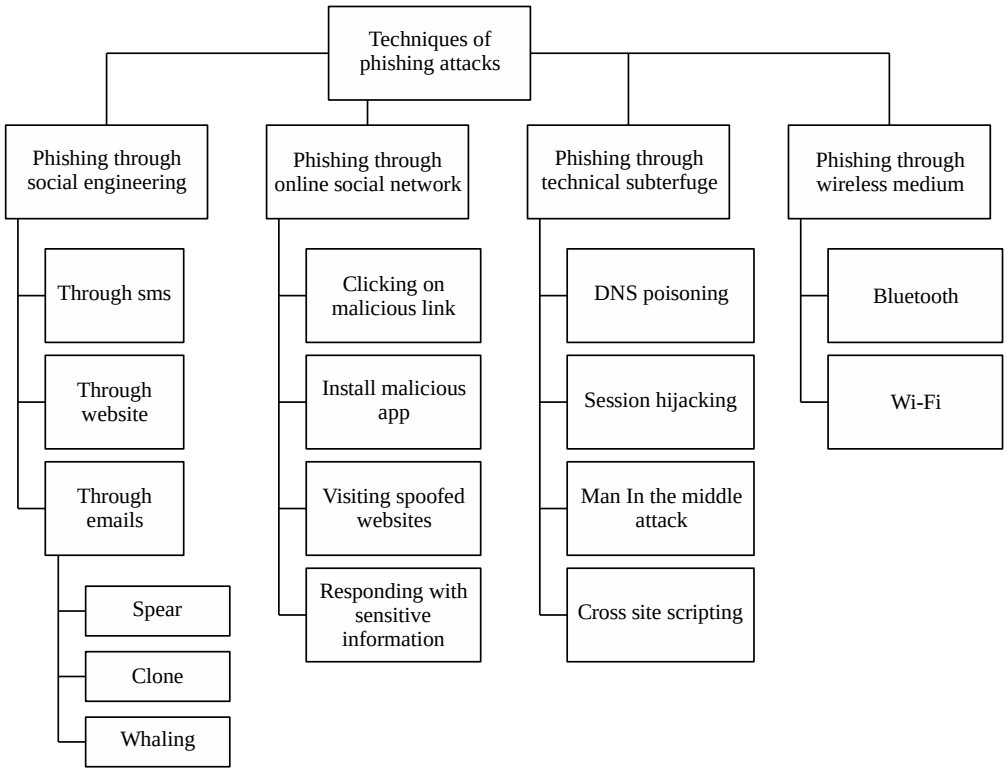

Figure 5. Taxonomy of email phishing

4.1. Phishing through social engineering

Sociology is termed as study of nature of human beings. Since a wider portion of malicious activities were consummated because of human errors and neglection. It requires cognitive manipulation in tricking users to get stuck in the trap and make security mistakes or giving away sensitive information [8]. It mainly depends on human error and lack of knowledge, rather than weakness in software and vulnerabilities in OS. Much less predictable mistakes often came from genuine users that are even hard to identify. Some of social engineering methods are discussed below:

4.1.1. Phishing through SMS

The process of stealing personal and financial information of person via sms is called Smishing [9]. This method is very common for doing phishing through mobile phones. Phishing is done by sending sms that contain malicious link or attachment that redirects the users towards a fake page to steal personal and financial information.

4.1.2. Phishing through websites

This method includes creating of malicious website that looks exactly same as the original website, for misguiding the users and stealing their personal information. The phishing websites can be a created one or a legitimate one containing malicious links.

4.1.3. Phishing through emails

This is the most common method of phishing these days since email communication is the widely used means of communication mainly in official purposes. The phisher sends fake mails or mails containing malicious link to the users in order to trick them and steal their personal, financial, login information. Email phishing is broadly categorized into three types:

- Spear phishing: In this type of phishing, attackers often gather user's personal information and use them to assure their success.
- Clone phishing: In this type of phishing attack, the attacker creates a clone of existing email and attach malicious content or link with the mail in order to steal person's info or any fraud. The email with malicious content is then sent to the victim that looks like it came from the original sender.
- Whaling: In this type, the phisher's attacks are directed specifically at person at higher level like the CEO of the company and other high-profile targets.

4.2. Phishing through online social network

Social networking sites are a craze these days. With these sites the users can interact, share ideas and stuff with each other. Millions of people spend a lot of time using these. The phishers took a good advantage of these social sites for their own advantage. Attackers are using these sites to initiate their attacks on a wide number of people via these social sites. Various incidents of fraud via social sites have been recorded. Various methods used by attackers to fraud users are listed below:

4.2.1. Clicking on malicious link

This is the most common way through which the users get trapped on the phishing attack. Phishers generate malicious links and spread them via these social sites to trap users. Such links help the phishers in completing their task by stealing user's information.

4.2.2. Installing malicious applications

Phishers built and upload malicious applications in form of games and value-added services on some sites and stores in order to steal and scan the user's data and information. These applications can be in the form of copy of original apps created by attackers.

4.2.3. Spoofed websites:

This attack is similar to that of malicious app attack, some of the most commonly successful scams are An Apple iTunes "emergency password reset" or a compromised Netflix account password reset [10].

4.2.4. Reveling sensitive information

Sometimes the most common and direct approach used by phishers is enough to gain sensitive information. A most common review reveals that about 30% students reveal their passwords in a university just on receiving a simple text message.

4.3. Phishing through technical subterfuge

Phishers uses this technique to gain or steal information from users for their personal benefits. Some methods used for technical subterfuge are discussed below:

4.3.1. DNS poisoning:

In this type of attack the users are redirected towards the malicious website by the attackers, and this is done by creating a fake DNS server or altering the existing one. In this attack the attacker takes advantage of vulnerability of domain name server.

4.3.2. Session hijacking

In this type of attack the main moto of phisher is to steal the security identifiers (SID) of the user in order to steal its credentials. SID is the session id that is provided by the application to authenticate the connection of the user. Once the SID is stolen, the attacker can now login into users account and steal information.

4.3.3. Man in middle attack (MITM)

It can be defined via an assumption of a mailman writing down your bank details and then delivering the envelope to you. In this attack the phisher places himself between the conversation of user and application for stealing user's personal and financial information.

4.4. Phishing through wireless medium

4.4.1. Bluetooth

Because of the flaw in devices having Bluetooth, that any other device can connect to them without their permission. This flaw can act as a big advantage for the phishers. The attacker can send any malicious link or file on devices with active Bluetooth connections.

4.4.2. Wi-Fi

Since Wi-Fi is a huge source of network these days. Many people didn't even authenticate to the access point resulting in insecure connection that act as an opportunity for the attacker to interrupt the communication and can even hijack the connection.

5. LITERATURE REVIEW

Many researchers have proposed various works on email phishing. Some of the proposed work are:

1. George et al. [11] in their work "Email Phishing Detection System Using Neural Network" has proposed a method of training based on neural network. They have used two datasets phish and ham data set, each consisting of 4500 emails. They have used various algorithm like FNN with back propagation algorithm for training and identifying ham and phish emails, fist order statistical measures for finding out the best features from the extracted ones. This has achieved a very low false negative and false positive rate. 99.95% was the best classified result achieved using 12 best features.
2. The authors in their work "Identification and Detection of Phishing Emails Using Natural Language Processing Techniques" [12] has focused on detecting phishing emails that do not contain any links and urls. They have on focused on email communication. They make use of NLP and WordNet in their proposed work. They have examined over 600 phishing emails and 400 genuine emails and collected a list of features like absence of recipient's name, asking for money or mention of money, a sense of urgency, inducing sentences that lure the victim to reply them. They have used Stanford Core NLP's (natural language processing) application program interface for forming a base for all the words present in phishing email. TN (true negative), FN (false negative), FP (false positive), TP (true positive) are used for detecting the quality of their proposed work. Their obtained results are TN=398, FN = 4, FP= 2, TP= 596. Their future work is to improve the accuracy. They will be using RiTa(Real Intelligence Threat Analytics)[13] WordNet API for programmatically accessing of databases and Optical Character Recognition techniques for performing the phishing detection on the text contents obtained from image form attachments sent in mails.
3. Yasin and Abuhasan [14] in their work "An intelligent classification model for phishing email detection" has proposed a classification model using intelligent preprocessing phase for the extraction of various features of email like email header, body, terms and frequency, by applying the techniques of data mining and knowledge discovery for phishing emails or spoofed emails. WordNet ontology was used to enrich the features and for enhancing the similarity between emails messages, text preprocessing technique of stemming is used. For training and testing of model two accredited data sets (phishing and ham emails) and 10-fold cross validation techniques were used in testing and training process. Very popular data mining algorithms like random forest, J48, Bayes net SVM and MLP were used to experiment the model. Highly encouraging classification results with high accuracy rates were obtained as compared to previous models.
4. Qbeitah and Aldwairi" [15] in their work "Dynamic Malware Analysis of Phishing Emails" has proposed a methodology for dynamic analysis and for capturing new malware samples and understanding their behave w.r.t files, registry, OS and network. They have designed a lab using three Dionaea honeypots for capturing the malware samples and for analyzing those captured samples a lab using REMNUX sandbox was setup. They examined ".exe" and "excel file" (from UAE based organization) from the newly captured malware samples and presented a detailed analysis on them using REMNUX. Their work contributed a lot in response procedures by malware analysts.
5. "Detection of phishing attacks" by Baykara and Gürel [16], in their work they have developed an application "Anti Phishing Simulator" to identify and detect the phishing element in text and message using the Bayesian classification algorithm with many databases. New phishing/spam word and urls can also be added to the database using "add spam" feature. The generated application focuses on preventing violation by controlling security and checking the incoming mail to ensure whether it contains any malicious content. Spam box is used for storing spam mails and is also user friendly.
6. The authors in their work "An approach for Malicious Spam Detection in Email with comparison of different classifiers" [17] proposed a model for performing feature selection of phishing emails by employing a novel dataset using two models NB, SVM classifier. A training dataset and a test dataset containing 702 spam/ham mails and 260 mails (130 spam and 130 non-spam emails). The author has used scikit-learn Machine Learning library (an open source python machine learning library) for classifier's training. The obtained result shows that both the models have balanced false positive in SVM (support vector machine) and a similar performance rate on test-set.

7. Damodaram [18], in her work **"**study on phishing attacks and antiphishing tools" determines various concepts of phishing, types of phishing attacks, its life cycle, and has given a brief discussion of various anti-phishing tools:
   - "Mail-SeCure" (it is a module that combines various technologies like anti-phishing database, SURBL (Spam Uniform Resource Identifier Real-time Block List) [19], Commtouch RPD, Heuristic Fraud detection sets of rules, internet protocol (IP) reputation, rate limit.
   - Netcraft "A Security Tool Bar"
   - "Set Security"
   - "Browser Integrated Tools"
   - "Using Anti-phish and Dom Anti-phish Techniques".

The author's study has given an awareness about the phishing problems and solutions.

6. SOLUTION APPROACH/ METHODOLOGY USED

A lot of works have been done by the researchers in email classifications, detection and preventions using many techniques. Our focus is on classifications of phishing emails using machine learning techniques. The dataset "The Short message service Spam Collection v.1" consisting of 5,574 tagged (ham/spam), real and non-encoded English messages [20] has been used for classification. Natural Language Processing, and machine learning classifiers were used for classification. Text classification and analysis of phishing datasets has been done using NLP concepts, scikit-learn and NLTK. Various classifiers like SVC, Decision Tree, and Random Forest KNeighbors Classifiers are used.

NLP: NLP stands for Natural language Processing. It is defined as a field of AI that helps computer to communicate with humans. Because of NLP, it becomes possible for the computers to read, hear, edit and interpret text, speech and determine which parts are important. Basic NLP tasks include: removing stop words, punctuations, special characters, tokenization, stemming, tagging, language detection and identification of semantic relationships. It is also explained as the means of handling the natural language by automatic means using a software. Basic NLP tasks include: removing stop words, tokenization, part-of-speech tagging, stemming, punctuations, special characters, language detection and identification of semantic relationships. Scikit-learn is a machine learning library for the Python programming language. Various classification, regression and clustering algorithms are also defined in this library. It is a library in Python that provides many unsupervised and supervised learning algorithms [21]. It's built upon some of the technology you might already be familiar with, like NumPy, pandas, and Matplotlib. NLTK is termed as a "wonderful tool for teaching, and working in, computational linguistics using Python," and "an amazing library to play with natural language". This platform allows to work with data that is in form of human language by building python programs. NLTK is embedded with various text processing libraries and easy-to use interfaces to over 50 corpora and lexical resources [22].

This analysis is done using anaconda jupyter lab. The coding is done using python. The working procedure is as per following steps:

- Downloading spam and phishing datasets.
- Opening the jupyter lab on the same folder where the datasets are located, using anaconda prompt.
- Now start with code writing that involves various steps:
- Importing libraries
- Load the dataset and reading the content (text files).
- Preprocessing of dataset: the very first step in NLP that involves tokenization, stop words, stemming, removing numbers and punctuations.
- Generating features and creating a feature set.
- Dividing the feature set into training and testing datasets.
- Importing chosen classifiers from sklearn and applying them on the testing dataset for computing the accuracy score.
- Lastly representing results using confusion matrix and classification report.

The Classification of dataset is done by building python code using the anaconda jupyter lab. Following are the steps involved in classification procedure, as shown in Figure 6.

1. **Import Necessary libraries**: The very first step is importing the necessary libraries. The imported libraries are os, glob, python, pandas, numpy, nltk, sci-kit, sent_tokenize, word_tokenize, Porter Stemmer, Counter, model_selection, Sklearn Classifier, SVC(support vector classifier), KNeighbors Classifier[23], Decision Tree Classifier, Random Forest Classifier, classification_report, accuracy_score, confusion_matrix, Logistic Regression. Further can be added when required.
2. **Load the Dataset:** Python pandas have been used for reading the dataset. To use particular dataset, open the jupyter lab in that database's location using the anaconda prompt.

3. **Preprocessing of Data:** The very first step in classification process is the preprocessing of dataset. This includes converting whole text in lower case, removing numbers, web address, and punctuations, removing stop words, tokenization, stemming.
4. **Features Generation:** this is an important step in classification. Feature engineering is used to generate features from the dataset using domain knowledge and those features will be used by machine learning algorithms. The features are in forms of tokens that are generated in the previous step. A feature set is created from these features that consists of the most common features. The feature set can also contain features that are not meaningful or of very short length, such features need to be removed for better results.
5. **Generation of Datasets for Testing and Training the Model**: The feature set is divided in equal or any ratio as per our concern to make training and testing datasets. The training dataset is used for training the classifiers or building a model. While a testing dataset is used for validating the built model and calculating the results.
6. **Applying Classifiers:** Classifiers, algorithms that have to be used for classification need to be imported. Various sklearn classifiers have been used.
7. **Results:** Calculating the accuracy rate of all the classifiers and creating the classification report and confusion matrix. The accuracy rate calculated by the K Nearest Neighbors classifier is 94.75, Decision Tree classifier is 97.55, Random Forest classifier is 98.42, Logistic Regression classifier is 98.56, SGD Classifier is 98.34, Naive Bayes classifier is 98.70, and SVM Linear classifier is 98.77, as shown in Figure 7.

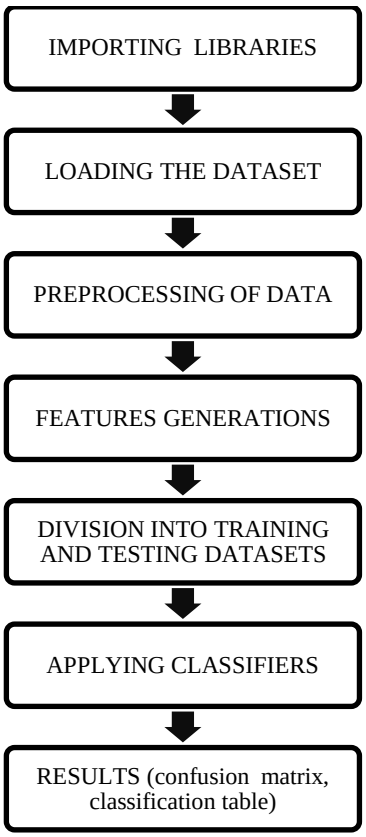

Figure 6. Working procedure

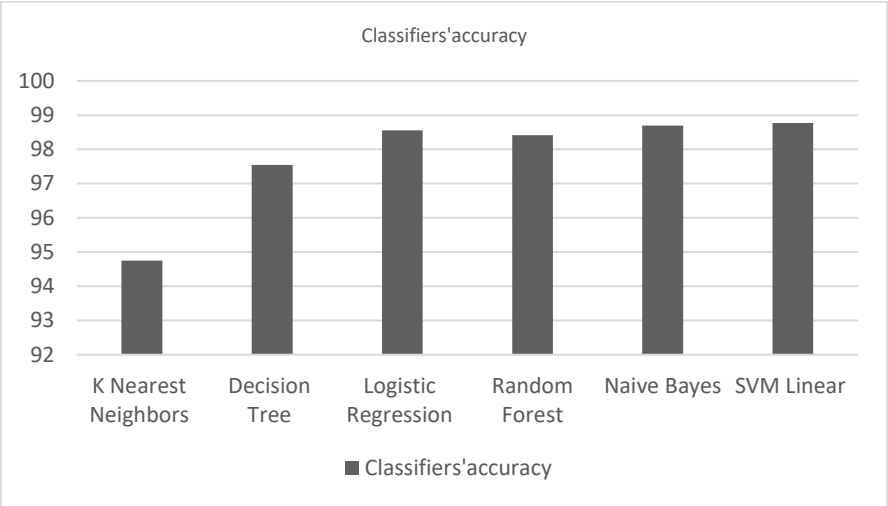

Figure 7. Showing calculated accuracy rates

Classification report: This report displays the precision, recall, F1, and support scores for the model as shown Table 1. Precision is termed as the ratio of TP to the total of TP and FP. It states from all the positively classified instances which percent are actually correct. Recall is defined as the ability of the classifier to find all the positive instances. It states what percent of instances are classified correctly, that were actually positive. It is the ratio of TP to the sum of TP and FN. F1-score is calculated by taking the mean of recall and precision. The best score is denoted by 1.0 and 0.0 for worst score. Support defines the actual occurrences of the classes in the dataset. Any structural weakness in the score can be indicated by imbalanced support.

Table 1. Classification report

	Precision	Recall	F1-score	Support
0(ham)	0.99	1.00	0.99	1208
1(spam)	0.99	0.93	0.96	185
Micro average	0.99	0.99	0.99	1393
Macro average	0.99	0.96	0.98	1393
Weighted average	0.99	0.99	0.99	1393

Prediction/confusion matrix: the performances of the classification algorithms is summarized using the confusion matrix. Confusion matrix shows the way in which our model is confused when it makes prediction. It gives a better idea of what types of mistakes our model is making. The calculated confusion matrix as show in Table 2.

Table 2. Confusion matrix

Actual/predicted	ham	spam
ham	1206	2
spam	13	172

7. CONCLUSION

Email phishing is the act of tricking the mail recipient business or any other entity in order to obtain sensitive personal information by sending fake mails and making the receiver believe that it came from a genuine source. User education and awareness is must for fighting against such big issue. This paper gives a detailed description on the classification of phishing emails using the natural language processing concepts. The calculated accuracy rates of classifiers are good, the classification report and the prediction matrix are also generated. There is a huge scope for the research in this area. The future work will be working on big raw and unstructured dataset for classification and clustering.

REFERENCES

[1] https://en.wikipedia.org/wiki/Phishing
[2] https://www.proofpoint.com/us/corporate-blog/post/2019-state-phish-report-attack-rates-rise-account-compromise-soars
[3] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf
[4] https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
[5] Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE communications surveys & tutorials*, *15*(4), 2070-2090.
[6] https://heimdalsecurity.com/blog/abcs-detecting-preventing-phishing/
[7] Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security*, *73*, 519-544.
[8] https://www.incapsula.com/web-application-security/social-engineering-attack.html
[9] Kang, A., Lee, J. D., Kang, W. M., Barolli, L., & Park, J. H. (2014). Security considerations for smart phone smishing attacks. In *Advances in Computer Science and its Applications* (pp. 467-473). Springer, Berlin, Heidelberg.
[10] https://www.revealrisk.com/2019/02/20/deep-sea-phishing-a-taxonomy-for-email-threats/
[11] Abdullah, A. A., George, L. E., & Mohammed, I. J. (2015). Research Article Email Phishing Detection System Using Neural Network. *Research Journal of Information Technology*, *6*(3), 39-43.
[12] Aggarwal, S., Kumar, V., & Sudarsan, S. D. (2014, September). Identification and detection of phishing emails using natural language processing techniques. In *Proceedings of the 7th International Conference on Security of Information and Networks* (p. 217). ACM.
[13] https://isc.sans.edu/forums/diary/Using+RITA+for+Threat+Analysis/23926/
[14] Yasin, A., & Abuhasan, A. (2016). An intelligent classification model for phishing email detection. arXiv preprint arXiv: 1608.02196.
[15] Qbeitah, M. A., & Aldwairi, M. (2018, April). Dynamic malware analysis of phishing emails. In *2018 9th International Conference on Information and Communication Systems (ICICS)* (pp. 18-24). IEEE.
[16] Baykara, M., & Gürel, Z. Z. (2018, March). Detection of phishing attacks. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-5). IEEE.
[17] Sah, U. K., & Parmar, N. (2017). An approach for malicious spam detection in email with comparison of different classifiers.
[18] Radha Damodaram (2016). Study on phishing attacks and antiphishing tools, IRJET.
[19] https://help.returnpath.com/hc/en-us/articles/220220208-What-is-the-Spam-Uniform-Resource-Identifier-Real-time-Block-List-SURBL-
[20] https://archive.ics.uci.edu/ml/datasets/sms+spam+collection
[21] https://en.wikipedia.org/wiki/Scikit-learn
[22] https://www.nltk.org/
[23] Brownlee, J. (2016). K-Nearest Neighbors for Machine Learning. *Machine Learning Mastery*, *15*.