Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 5196- 5203
Received 15 May 2021; Accepted 20 May 2021.

An Adaptive and Dynamic Methodology for Detecting Phishing Email Based on Artificial Intelligence

Ms. K. Narmatha[1], Mr. T Srikanth[2], Mr. Maheshraj R P[3], Mr. Sanjay B[4]
[1,2,3,4] SRM Institute of Science and Technology Ramapuram Campus, India

*mp3993@srmist.edu.in

ABSTRACT

Phishing is an exploit method that is used to steal information from a targeted individual or an organization by impersonating legitimate sites. This paper can detect such targets and warn the users. Classified mails are used to train the classifier for classifying the email and the others are used for testing the derived classifier model. The feature vector of the training set is trained by extracting and breaking down elements from the mail. Training is done so as to obtain required classifier model which is then used to classify the mail into an phishing email or not. The main objective of this project is detecting phishing through email address separation. This phishing detection method is found to be effective against various targeted phishing attacks. The proposed system is able to check and verify the phishing emails that usually target in large numbers by impersonation of a particular organization so as to be able to gain access to their resources by flagging them as phishing mail or not.

Keywords
Phishing, exploit, target, email, check.

Introduction

The world is currently on to the digital era where every detail, every document, every information is stored in digital formats. These files are too crucial to fall into wrong hands. When enough precaution is not taken, these documents can fall into the wrong hands and thereby giving them enough power that can even destroy an entire organization. Thus, it is necessary to take precautions against losing this crucial information. There are many ways that data theft can occur. One such is ‘phishing’.

Figure. 1. An image representation of card info theft

In this method know as phishing, individuals target a user or an organization who are uninformed about the existence of such data theft methods, and thus, they prone to these methods such as phishing. The phishing method is of many types ranging from hooking sensitive credentials to installing malicious malware in the client's system. Phishing can be defined as an attempt with a malicious intent to collect sensitive data or information which are usually an end user account's credentials, credit card numbers by creating a fake entity of another entity that usually requires this information that are usually gathered by email, text messages and other forms of communications. There have been many incidents where phishing proved to be one of the dangerous digital attacks that could ever happen. Phishing attacks could target users for instances ranges from monetary benefit to personal vengeance. The losses that could be incurred by phishing attacks could range from few dollars to billions based on the attack and depending on the end user.

Since, the phishing method is deployed usually via mail and other forms of communications such as social media, instant messaging services, ads, etc. Thus, a suitable model that would be able to detect such malicious attacks and a model that can warn the user to tread carefully as the mail or the form of communication is suspicious arises.

Our model can satisfy such needs and can safeguard the user from such malicious attacks. This research paper uses messages that consist of two parts i.e. one for classifier training and other for testing. Once trained and tested, that model is used in classification of phishing messages.

An Adaptive and Dynamic Methodology for Detecting Phishing Email Based On Artificial Intelligence consists of methods that would be able to effectively track phishing mails and warn the user.

The Dynamic Methodology for Phishing Detection (DMPD) model is able to identify the phishing content in a webpage. It is able achieve this by the undergoing various processing that includes Data analysis, preprocessing of data, model training and testing of Dataset.

Literature Review

In a phishing attack mail, approaches such as sender centric phishing mail detection has an increased phishing detection mechanism than the one with the content centric phishing mail detection system which is developed by Fernando Sanchez and Zhenhai, Duan[1]. Also, in content centric phishing mail detection system, mechanism such as Themis model which is developed by Yong Fang, Cheng Zhang, Cheng Huang , Liang Liu, And Yue Yang, is able to reach accuracy to level as high as 99.848%[2]. Also, the false positive rate of the mechanism is found to be 0.043%. This also proves to be a very low false positive rate.[2]

Phishing attacks are conducted on various types of platforms and mechanisms. Knowing the common types of phishing methods would be greatly helpful in devising a phishing detection system. The most common phishing attacks would be :- Email Phishing, Angular Phishing, Whaling, Spear Phishing, Whaling[3]. It is necessary to devise a method that would be able to counter such commonly deployed phishing attacks.

A Sender-Centric Approach to Detecting Phishing Emails, Fernando Sanchez and Zhenhai, Duan. Here, the process is divided into two steps. In the first step, all the emails received are segregated into two categories, namely, banking and non-banking emails. Then, at the second step, for all banking emails the path of the sender is verified and compared with the bank from which it is receiving and if the path doesn't match then the mail is classified as phishing email[1]. This system fails to acknowledge the point that most of the smaller banks are not registered for online banking and have hired other portals for online banking. Phishers can do the same by posing as a newly setup bank.

Phishing Email Detection Using Improved RCNN Model With Multilevel Vectors and Attention Mechanism, Yong Fang, Cheng Zhang, Cheng Huang , Liang Liu, And Yue Yang. This is the most advanced and most efficient systems proposed so far, for identifying phishing emails by using RCNN for image processing and attention mechanism identify the contents of the processed image The Themis model proposed in this system, considers the whole email as an image and processes it to identify the textual contents of the image[2]. But what this systems lacks is that, emails now have the ability to attach pictures in the body of the email, due to this, hyperlinks can be attached to that images in the form of click button to take the user to another webpage and this system cannot read the hyperlink attached to the click button in the image.

Email Anti-Phishing Detection Application, Rabab Alayham Abbas Helmi, Chua Shang Ren, Arshad Jamal. This is a research paper that presented a detailed an analysis and report on the types of phishing techniques employed by the phishers, who are the targets of the phishers, how the phishing affects the users and the existing methods to tackle the phishing problems. From the existing anti phishing measures, this research has suggested a few trustable applications that were effective against phishing attacks [3].

Detection method of phishing based on persuasion principle, XueLi ,Dongmei Zhang , Bin Wu. In this method, a model is constructed by using machine learning to detect phishing emails. The model is trained by sampling certain parameters like the proper format of a URL, the domain of the link, IP address attached to the link, pop-ups attached to the link and the further details and the using these details a comparison is made with the contents of the mail and is flagged if specified details doesn’t match[4]. The major drawback of this system is that it is continuously learning and anytime a new type of phishing email that is not previously registered, then the system fails and leaves a vulnerability for a phishing attack.

Multilayer hybrid strategy for phishing email zero-day filtering, M.U. Chowdhury, J.H. Abawajy, A.V. Kelarev. A divide and conquer approach is followed in this model, where the email is divided into subsets based on the structure of the email and these subsets are further divided and a series of data pruning is run to eliminate the unwanted data and separate the required data by training the model to identify the targeted elements in the email. Then the elements are then checked and compared with the pre-loaded or a structured data for identifying the cues for the possible phishing entities. Then the emails are flagged into respective categories and updates the user[5]. Though this model is efficient, it still has room for improvements. The time span for getting the outcome is high and can sometimes have lags. The data has to be retained every time, when a new data is found and the data filtering accuracy decreases every time a new data set is encountered as phishers do not always use the same methods for phishing.

Moreover, this model requires mathematical corrections and needs to be reviewed mathematically for decreasing the time lag.

Proposed Model

Phishing is defined as one of the many dangerous computer attacks in which an attacker usually an individual creates a masqueraded website of a legit organization in order to trick the targets into giving out credentials. They can also target and trick clients to install malware onto their systems. People targeted by phishing attacks can lose money, credibility, access to computer resource and a lot more based on the attacker’s motive. Phishing consist of various methods to deceive the users. In this paper, the considered method is email. This paper is useful in cases where an attacker uses email as a medium to fake.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 5, 2021, Pages. 5196- 5203
Received 15 May 2021; Accepted 20 May 2021.

In this phishing detection method, context plays a very important role for detection. The proposed model instead of considering mail as a single entity breaks down the email into tokens. These tokens are then considered as the variables or the deciding factor for the email classification to occur.

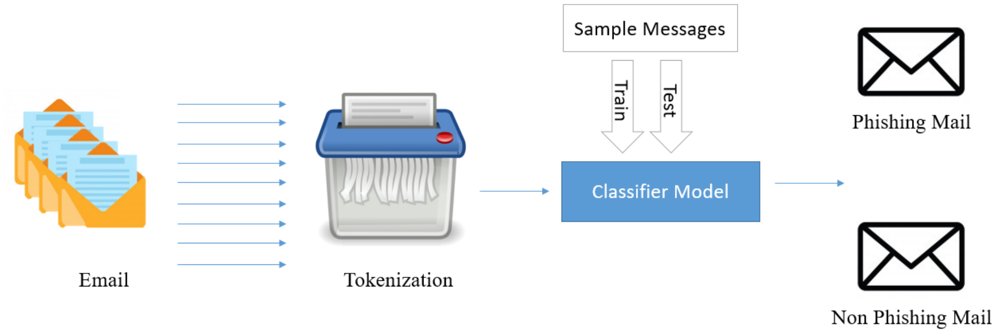

Figure 2. DMPD Flow Chart

The proposed system is found to reduce the hardware resource consumption, also it is easy to merge with the existing email systems so as to detect the threatening phishing emails, provided the systems are optimized and involves less computation time. It can be described as the one of the few accurate algorithms. When worked with large number of datasets the accuracy is found to higher. It also works efficiently with multiple large databases.

DMPD Algorithm

The DMPD Algorithm i.e. Dynamic Methodology for Phishing Detection is devised in such a way to identify the phishing mails that could harm the end users with an increased success rate than the pre-existing models and thus, it consists of two methods working together. It uses various steps to achieve this. The following flow chart gives a detailed explanation regarding the steps involved in the DMPD Algorithm.

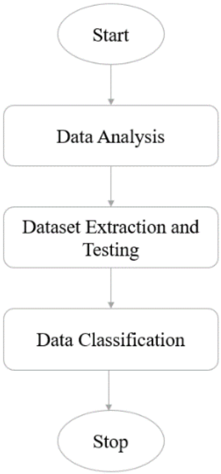

Figure 3. DMPD Algorithm

The DMPD Algorithm consist of the above process: - It is further explained below.

1. Start
2. Analysis of Data
3. Data Extraction
4. Separation of Data for Training Model and Testing
5. Data Classification using Trained Model
6. Stop

Modules

Data Exploration

As the module name say's – Data Exploration, in this module, we analyze the input data. In Text Processing, the exploratory analysis of data is the process by which data is went through and is searched thoroughly to find patterns and information present in them. In order perform such data exploration we depend on tools such as Database Management System, Data Mining tools, statistical analysis packages, etc. These tools act vital in the Data Exploration module. In the data exploration, we perform the perform the training of the AI. Multiple phishing mails are fetched to model. This helps in devising the classifier model. Building classifier model is important as the classifier model takes the sole responsibility for the classification of email elements. The classifier model is first trained. The classifier model then enters the testing phase once is found to be trained enough, During the phase, the classifier model is put through multiple test to classify emails. Thereby again building the classifier model, which is key important in verifying the credibility of the mail such as a phishing email or not.

Text Preprocessing

In Text Pre-processing module, we execute pre-processing steps before the classification. This method uses StanfordNLP library to perform pre-processing operation. This method breaks down the sentences into word vectors that are need to processed for classification. It uses information from general grammar such as parts of speech, linguistic annotations for text, sentence boundaries, token, etc. for breaking down to tokenizing the words. In short Pre-processing involves tokenizing of sentences to make it classifier model ready. The sentences are broken down into multiple tokens before the classification could commerce. In pre-processing, all punctuations are ignored except punctuations such as exclamation, full stop, comma, question mark, etc. These punctuations are kept so as to understand the sentence that would assist while the tokenization process occurs. Also case folding is a part of pre-processing. Case Folding is defined as the process of converting words into even case.

Classification Technique

This module makes use of the classifier model obtained from the data exploration model. The classifier model obtained helps in classifying the input emails as phishing ones or not. This classification is done with the help of ham and spam flags. Since, the words are tokenized, a far efficient method to arrive at classification is achieved. Only a fraction of every mail makes the email term as phishing or not and hence tokenization of elements in a mail targets finding this fraction. It employs tokens derived from the training and uses it in classifying emails as phishing emails.

Implementation

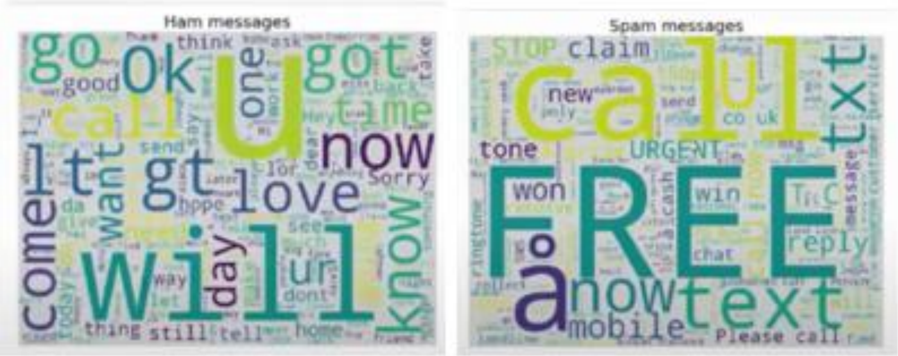

Figure4. Segregation of Ham and Spam using Python Script

The proposed theory is put into action with the help of a Python Script that is able to segregate between two flags i.e. Ham and Spam as shown in the above figure. This implementation converts email into tokens and then implements its algorithm. Every email is divided into multiple parts and of these only few parts makes the email as an phishing email. Tokenization of email helps in finding these parts as the email uses StanfordNLP Python Library that removes unnecessary words and focus on what’s necessary. Thus, after spotlighting key important tokens and using the classifier model that is trained and tested, one can be able to flag the email as phishing or not. The algorithm is able to flag the email as phishing or not by using these Ham or Spam flag and using the threshold level of these flags the system marks the email. This python script can be employed along with software to get the prediction.

Result

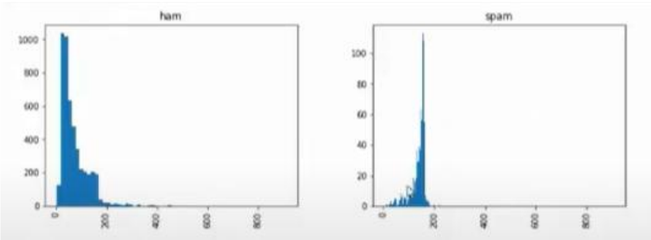

Figure 5. Graph Representation of Ham and Spam

Thus, by employing this algorithm one is able to get the suitable count as shown in the above figure and using the threshold value one is able to classify the mail.

Thus, a fast efficient method to detect phishing email is devised. This approach is considered to fast and efficient because of the tokenizing process as the email is tokenized and the sentences that prove to be of very less importance is removed and thus focusing on the parts that are really vital. Since the word count is drastically reduced the algorithm can work on the email faster. This

then followed by the classification using the classifier model . The classifier model is trained and tested for this classification of the phishing detection. Thus, phishing detection is achieved.
This devised system can be developed to be an addon to the existing mailing systems since it's just a python script. Provided this system can also be converted into full-fledged software that would be able to work alongside the mailing systems and achieve phishing detection.

Conclusion

The proposed system can also be programmed to detect spam too as tokenization process is also found to be an efficient way to flag for spam emails. A Phishing and Spam detection system using tokenization could be devised. There's a vast scope for this tokenization system as this system could show a brief overview of the email thereby helping the user read the entire email with just a glanze. These features can be bundled into a single system making the system function in an fast and effective manner. This would be the future work scope for our proposed model

References

[1] F. Sanchez and Z.Duan (2019).A Sender-Centric Approach to Detecting Phishing Emails, CYBERSECURITY '12: Proceedings of the 2012 International Conference on Cyber Security.

[2] Y. Fang, C. Zhang, C. Huang, L. Liu, And Y. Yang (2019, April),Phishing Email Detection Using Improved RCNN Model With Multilevel Vectors and Attention Mechanism, , IEEE Access, Volume: 7, Pg. 56329 – 56340.

[3] R. A. A. Helmi, C. S. Ren, A. Jamal (2019, October), Email Anti-Phishing Detection Application, 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET).

[4] X.Li ,D. Zhang , B. Wu (2020, October), Detection method of phishing based on persuasion principle, 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC).

[5] M.U. Chowdhury, J.H. Abawajy, A.V. Kelarev (2021, January),Multilayer hybrid strategy for phishing email zero-day filtering, Concurrency & Computation Practice & Experience, Vol. 29, Issue No. 23, Pg. 56-74.

[6] J. D. Ndibwile, E. T. Luhanga, D. Fall, D. Miyamoto, G. Blanc and Y. Kadobayash (2019, September),An Empirical Approach to Phishing Countermeasures Through Smart Glasses and Validation Agents, IEEE Access, Volume: 7, Pg. 130758 - 130771.

[7] R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach and A. Shabtai (2018, March) Taxonomy of mobile users' security awareness, Computers and Security, Volume: 73, Pg. 266-293.

[8] M. Jensen, A. Durcikova and R. Wright (2017),Combating phishing attacks: A knowledge management approach, Proc. Hawaii International Conference on System Sciences, Pg. 1-10.

[9] E. Kritzinger and S. von Solms (2012), A framework for cyber security in Africa, The Journal of Information Assurance & Cybersecurity, Volume: 2012, Pg. 1 - 10.

[10] L. Wu, X. Du and J. Wu (2016, August),Effective defense schemes for phishing attacks on mobile computing platforms, The IEEE Transactions on Vehicular Technology, Volume: 65, Pg.6678-6691.

[11] Luke Irwin (2020, April), The 5 most common types of phishing attack, https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack.

[12] C. Yue and H. Wang (2008, December), Anti-phishing in offense and defense, Proceedings of the Annual Computer Security Applications Conference, Pg.345-354.

[13] H. Shahriar and M. Zulkernine (2010, June), PhishTester: Automatic testing of phishing attacks, Proc. 4th Int. Conf. Secure Softw. Integr. Rel. Improvement, Pg. 198-207.

[14] J. S. Downs, M. Holbrook and L. F. Cranor (2007),Behavioral response to phishing risk, Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, Pg. 37-44.

[15] A. D. Veiga (2016),Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study, Information and Computer Security, Volume: 24, No. 2, Pg. 139-151.

[16] M. Jakobbson (2016), Understanding Social Engineering Based Scams, Springer.

[17] J. D. Ndibwile, Y. Kadobayashi and D. Fall (2017, August),UnPhishMe: Phishing attack detection by deceptive login simulation through an Android mobile app, The 12th Asia Joint Conference on Information Security(AsiaJCIS), Pg. 38-47.

[18] C. Pham, L. A. T. Nguyen, N. H. Tran, E. Huh and C. S. Hong (2018, September),Phishing-Aware: A Neuro-Fuzzy Approach for Anti-Phishing on Fog Networks, IEEE Transactions on Network and Service Management, vol. 15, no. 3, Pg. 1076-1089.

[19] L. Wenyin, G. Huang, L. Xiaoyue, X. Deng, and Z. Min (2005),Phishing Web page detection, Proc. IEEE 8th Int. Conf. Document Anal. Recognit., Seoul, South Korea, Pg. 560–564.