EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Email Phishing: An Enhanced Classification Model to Detect Malicious URLs

Shweta Sankhwar[1,*], Dhirendra Pandey[1] and R.A Khan[1]

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India

Abstract

Phishing is the process of enticing people into visiting fraudulent websites and persuading them to enter their personal information. Number in phishing email are spread with the aim of making web users believe that they are communicating with a trusted entity or organization. Phishing is deployed by the use of advanced and harmful tactics like malicious or phishing URLs. So, it becomes necessary to detect malicious or phishing URLs in the present scenario. Numerous anti-phishing techniques are in vogue to discriminate fake and the authentic website but are not effective. This research, focuses on the relevant URLs features that discriminate between legitimate and malicious/phishing URLs. The impact of email phishing can be largely reduced by adopting an appropriate combination of all these features with classification techniques. Therefore, an Enhanced Malicious URLs Detection (EMUD) model is developed with machine learning techniques for better classification and accurate results.

Keywords: Email, Phishing, Machine Learning Techniques, Information security, Cybercrime.

Received on DD MM YYYY, accepted on DD MM YYYY, published on 06 May 2019

doi: 10.4108/_____

1. Introduction

Over the last decade phishing attacks have grown considerably in the internet. E-mail Phishing is presently amongst the latest, very tricky and problematic of trends in network security threats. Phishing is a process of gaining the sensitive information of user through generating a fake or counterfeit webpage, which appears to be a legitimate one that actually comes under cybercrime. Malicious URL are challenging threat in cyber space which steals the user's sensitive information. Phishing is a serious threat that intent to use the vulnerabilities or weakness found in system process as caused by online users. Phishing refers to sending of spurious emails which are usually forged by the phishers to lure a user in their snares leading the user to lose sensitive data or credential, identity theft, pecuniary loss etc. Phishing URLs are challenging threat in cyber space which steal the user's sensitive information. The phishers are using numerous phishing URLs crafting tactics pointing to the same phishing website to bypass the detection techniques [1]. Therefore, it becomes necessary to detect the suspicious or malicious URLs in the present scenario. A lot of anti-phishing techniques are in vogue to draw a dividing line or identify between the fake and the authentic websites, however due to the vast amount and new harmful tactics of phisher, the challenges are yet being faced. [2] [3]

For instance, a system can be technically safe and secure enough against password theft, however naive users may leak their sensitive information if an attacker lead them to update their sensitive information such as username, passwords via a given Hypertext Transfer Protocol (HTTP) link [4]. It could ultimately breach the security of the system, web vulnerabilities like obfuscated/phishing URLs can be used by phishers to craft far more influencing socially-engineered messages. Fraudsters or phishers use spoofed domain names which can be persuading instead using legitimate domain names. [5] [6]

Therefore, to reduce the phishing attack Enhanced Malicious URL Detection (EMUD) model is developed

4.1.3 Comparation Study of Proposed and Existing Performance Metric

In this data analysis, confusion matrix is used to evaluate the performance of the proposed approach [24][25]. Here, the True Positive Rate (TPR) and False Positive Rate (FPR) is considered for evaluation [26]. In addition, we used standard measure i.e. Accuracy.

TP: Number of phishing URLs correctly classified as Phishing.
TN: Number of legitimate URLs correctly classified as legitimate.
FP: Number of legitimate URLs which are classified as phish
FN: Number of phishing URLs which are classified as legitimate
Here, the accuracy and performance are evaluated through confusion matrix as depicted in Table 5.

Table 5: Confusion matrix of EMUD and existing model

Model	Confusion Matrix		Result	
EPCMU	TPR	TP/(TP+FN)	6/6+7	6/13
	TNR	TN/(TN+FP)	2/2+0	1/1
	FPR	FP/(FP+TN)	0/0+2	0
	FNR	TP/(FN+TP)	7/7+6	7/13
	Accuracy	((TP+TN)/ (TP+TN+FP+FN)) *100	6+2/1 5	53%
EMUD	TPR	TP/(TP+FN)	13/13 +0	1/1
	TNR	TN/(TN+FP)	2/2+0	1/1
	FPR	FP/(FP+TN)	0/0+2	0
	FNR	TP/(FN+TP)	0/0+1 3	0
	Accuracy %	((TP+TN)/ (TP+TN+F P+FN)) *100	13/13 +0	100 %

Through this comparative analysis, EPCMU Classification Rate (%) is 53.3% and EMUD 100% Classification Rate which shows high accuracy in detection of malicious or phished URLs as shown in Table 5. In both the model i.e. EMUD and EPCMU employed NB classifier and it is also observed that the NB took long time for processing.
Therefore, in next section, some other ML techniques like SVM is employed for classification in the place NB in EMUD model.

4.2 Experimental Setup with Dataset-II

Dataset is collected from real world data of the 2000 phishing URLs and legitimate. Phishing URLs data source is Phishing tank (https://www.phishingtank.com) and legitimate URLs data source is DMOZ and Alexa (https://www.alexa.com/topsites). The EMUD algorithm test these data as input and employed machine learning to evaluate the accuracy and confusion matrix. The weka tool is used for the evaluation [27]. Specifically, the distribution ratio of phishing and legitimate data is in 60:40 ratio respectively. SVM classifier is used with confusion matrix and k-fold Cross validation (10-fold) is used for accuracy or performance evaluation.

4.2.1 Performance Evaluation with Support Vector Machine

In this experiment, Support Vector Machines (SVM) is adopted as it a popular classifier to achieve better classification. It is extensively used in text classification and specially in computer security field i.e. spam detection, hidden email construction, masquerade detection and phishing detection. The main benefit of this learning algorithm is that it is fully oblivious to the input feature numbers and focus to increase the separable margin [27] [28].

$$w' x_i + w_0 \_ 0 \text{ if } t_i = +1;$$
$$w' x_i + w_0 < 0 \text{ if } t_i = -1;$$

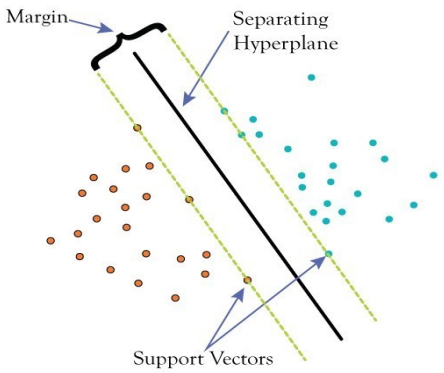

Figure 4. Support Vector Machine

Suppose that a linear discrimination function and two linear separable classes with target values +1 and -1. A discriminating hyperplane will satisfy, the distance of any point x to a hyperplane is |w' xi + w0| / ||w|| and distance to the origin is |w0 | / ||w ||. Support vectors are the points lying on the boundaries, and the middle of the margin is the optimal separating hyperplane that maximizes the margin of separation as shown in Figure 4. [28] [29][30]

4.2.2 Performance Metric

In this data analysis, we used confusion matrix to evaluate the performance of the proposed approach on which mainly the True Positive Rate (TPR) and False Positive Rate (FPR) is considered for evaluation as shown in Table 6. In addition, we used standard measure such as the Precision and Accuracy. [29] [31]

TP: Number of phishing URLs correctly classified as Phishing.
TN: Number of legitimate URLs correctly classified as legitimate.
FP: Number of legitimate URLs which are classified as phish
FN: Number of phishing URLs which are classified as legitimate [27]
Four metrics are calculated as follows:

True Positive Rate (TPR): It is the ratio of the phishing URLs that are correctly identified and the equation of the TPR is shown in eq. (5)

$$TPR = \frac{TP}{TP + FN}$$

True Negative Rate (TNR): It is the ratio of the legitimate URLs that are correctly identified and the equation of the TPR is shown in eq. (6)

$$TNR = \frac{TN}{TN + FP}$$

False Positive Rate (FPR): It is the ratio of the legitimate URLs that are classified as phishing and the equation of the FPR is shown in eq. (7)

$$FPR = \frac{FP}{FP + TN}$$

False Negative Rate (FNR): The number of phishing URLs classified as legitimate. The equation of the FNR is shown in eq. (8)

$$FNR = \frac{TP}{FN + TP}$$

Accuracy: The accuracy computation is shown in eq. (9)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision: The precision is defined as the number of true positive (TP) over the sum of True positive and False positive number is shown in eq. (10)

$$Precision = \frac{TP}{TP + FP}$$

Recall: The recall is defined as the number of true positive (TP) over sum of TP and FN is shown in eq. (11)

$$Recall = \frac{TP}{TP + FN}$$

F-1 Measure: The F1- Measure defined as the harmonic mean of precision and recall is given in the eq. (12).

$$F1 - Measure = 2\,\frac{precision * recall}{precision + recall}$$

Table 6. Performance for proposed model

Metric	TPR (%)	FPR (%)	Precision	Accuracy
EMUD with SVM	90%	4.90%	91.26%	93.01%

The EMUD algorithm test phishing emails by putting all as input and employed machine learning to evaluate the accuracy and confusion matrix. Specifically, the distribution ratio of phishing and legitimate data is in 60:40 ratio respectively. SVM classifier is used with confusion matrix and k-fold Cross validation (10-fold) is used for accuracy or performance evaluation. After using equation 5, 7, 9 and 10; the proposed EMUD model achieves 93.01% accuracy with 90% of True Positive (TPR) and 4.90% False Positive Rate (FPR) as shown in Table 6.

4.2.3 Comparative Study of Proposed and Existing Model

After using equation 5, 7, 9 and 10 the proposed model-EMUD achieved 93.01% accuracy. The same experiment is also done with existing model i.e. EPCMU with the same testing set.

Table 7. Comparison of proposed model with existing model

Approach	EPCMU	EMUD (Proposed)
TPR (%)	83.63%	90.90%
FPR (%)	13.8%	4.90%
Precision	85.8%	91.26%
Accuracy	84.58%	93.01%

EPCMU achieved 84% in second experiment with SVM classifier. It has high false positive rate in comparison to EMUD. The experiment results are shown in Table 7. Though this experiment, it is obvious that the SVM has better performance result and accuracy than others supervised learning techniques as shown in Table 6 and Table 7.

5. Conclusion

Phishing URLs are challenging threat in cyber space which steal the user's sensitive information. The phishers are using numerous phishing URLs crafting tactics pointing to the same phishing website to bypass the detection techniques. Therefore, a reliable mechanism i.e. Enhanced Malicious URLs Detection (EMUD) model is proposed to combat against aforesaid challenge. In this research paper, supervised machine learning techniques (i.e. NB and SVM) to detect malicious URLs with the EMUD algorithm has been used with EMUD model. EMUD model has more effective detection capabilities as it includes more detection parameter (relevant URL heuristics) to catch and detect malicious URLs in Comparation with other existing URL detection algorithm. But the NB classifier used is not appropriate as the processing time was long. Therefore, the SVM is applied with EMUD for classification and it is evident from experiment, that it has less time in processing and gives better accuracy & results in comparison to others supervised learning techniques. Hence, it is concluded that EMUD model detects the phishing/ obfuscated URLs more accurately with SVM. EMUD model can be more effective by adding latest pertinent heuristics for zero-day phishing detection. Adoption of artificial neural network methods could be more acceptable. Deep neural network will be more promising for phishing detection in terms of enhanced accuracy and performance with large dataset.

References

[1] Hong, Jason. "The state of phishing attacks." Communications of the ACM 55.1 (2012): 74-81.

[2] Shah, Ripan, et al. "A proactive approach to preventing phishing attacks using Pshark." Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference on. IEEE, 2009.

[3] Zhang, Yue, Jason I. Hong, and Lorrie F. Cranor. "Cantina: a content-based approach to detecting phishing web sites." Proceedings of the 16th international conference on World Wide Web. ACM, 2007.

[4] Zhang, Jian, Phillip A. Porras, and Johannes Ullrich. "Highly Predictive Blacklisting." USENIX Security Symposium. 2008.

[5] Sankhwar, Shweta, Dhirendra Pandey, and R. A. Khan, "Phishing: A Critical Review", International pure Applied and Mathematics, ISSN: 1314-3395, Vol. 119 No. 15. 2018, pp. 2917-2923.

[6] Center, RSA Anti-Fraud Command. "RSA monthly online fraud report." (2012).

[7] Sankhwar, Shweta, and Dhirendra Pandey. "Defending Against Phishing: Case Studies." International Journal of Advanced Research in Computer Science 8.5 (2017).

[8] N. Chou, et al.," Client-side defense against web- based identity theft," in In Proc. 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego, CA., 2004.

[9] McGrath, D. Kevin, and Minaxi Gupta. "Behind Phishing: An Examination of Phisher Modi Operandi." LEET 8 (2008): 4.

[10] Sankhwar, Shweta, Dhirendra Pandey, and R. A. Khan, "A Glance of Anti- Phish Techniques" International pure Applied and Mathematics, ISSN: 1314-3395, Vol. 119 No. 15. 2018, pp.2925-2936.

[11] Chandrasekaran, Madhusudhanan, Ramkumar Chinchani, and Shambhu Upadhyaya. "Phoney: Mimicking user response to detect phishing attacks." Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks. IEEE Computer Society, 2006.

[12] Zhang, Yue, Jason I. Hong, and Lorrie F. Cranor. "Cantina: a content-based approach to detecting phishing web sites." Proceedings of the 16th international conference on World Wide Web. ACM, 2007.

[13] Fette, Ian, Norman Sadeh, and Anthony Tomasic. "Learning to detect phishing emails." Proceedings of the 16th international conference on World Wide Web. ACM, 2007.

[14] Sankhwar, Shweta, and Dhirendra Pandey. "A Comparative Analysis of Anti-Phishing Mechanisms: Email Phishing." International Journal of Advanced Research in Computer Science 8.3 Volume 8, No. 3, March – April 2017 (2017).

[15] Suriya, R., K. Saravanan, and Arunkumar Thangavelu. "An integrated approach to detect phishing mail attacks: a case study." Proceedings of the 2nd International Conference on Security of Information and Networks. ACM, 2009.

[16] Sankhwar, Shweta, Dhirendra Pandey, and R. A. Khan. "A Step Towards Internet Anonymity Minimization: Cybercrime Investigation Process Perspective." Information and Decision Sciences. Springer, Singapore, 2018. 257-265.

[17] Center, RSA Anti-Fraud Command. "RSA monthly online fraud report." (2012).

[18] J. Yearwood, et al.," Profiling Phishing E-mails Based extracted from emails," in Soc. Netw. Anal. Min. (2012) 2:5–16

[19] Jayakanthan, N., A. V. Ramani, and M. Ravichandran. "Two phase Classification Model to Detect Malicious URLs." International Journal of Applied Engineering Research 12.9 (2017): 1893-1898.

[20] Harrington, Peter. "Machine learning in action." Shelter Island, NY: Manning Publications Co (2012).

[21] Lotte, Fabien, et al. "A review of classification algorithms for EEG-based brain–computer interfaces: a 10 year update."Journal of neural engineering 15.3 (2018): 031005.

[22] Manik Sharma, Samriti Sharma, Gurvinder Singh. "Performance Analysis of Statistical and Supervised Learning Techniques in Stock Data Mining". Data 2018, 3, 54.

[23] Kaur, Loveleen, and Ashutosh Mishra. "An Empirical Analysis for Predicting Source Code File Reusability Using Meta-Classification Algorithms." Advanced

Computational and Communication Paradigms. Springer, Singapore, 2018. 493-504.
[24] Gomez, Juan Carlos, Erik Boiy, and Marie-Francine Moens. "Highly discriminative statistical features for email classification." Knowledge and information systems 31.1 (2012): 23-53.
[25] A. G. K. Janecek and W. N. Gansterer, ``E-mail classification based on NMF," in Proc. 9th SIAM Int. Conf. Data Mining (SDM), Sparks, NV, USA, 2009, pp. 1345_1354.
[26] Gansterer, Wilfried N., and David Pölz. "E-mail classification for phishing defense." European Conference on Information Retrieval. Springer, Berlin, Heidelberg, 2009.
[27] Abu-Nimeh, Saeed, et al. "A comparison of machine learning techniques for phishing detection." Proceedings.
[28] Manik Sharma, Gurvinder Singh, Rajinder Singh. "Accurate Prediction of Life Style Based Disorders by Smart Healthcare Using Machine Learning and Prescriptive Big Data Analytics." Data Intensive Computing Applications for Big Data 29 (2018): 428.
[29] Sokolova, Marina, and Guy Lapalme. "A systematic analysis of performance measures for classification tasks." Information Processing & Management 45.4 (2009): 427-437.
[30] Sankhwar, Shweta, Dhirendra Pandey, and R. A. Khan. "A Novel Anti-Phishing Effectiveness Evaluator Model." International Conference on Information and Communication Technology for Intelligent Systems. Springer, Cham, 2017.
[31] Sharma, M., G. Singh, and R. Singh. "Stark Assessment of Lifestyle Based Human Disorders Using Data Mining Based Learning Techniques." IRBM (2017).