PalArch's Journal of Archaeology
of Egypt / Egyptology

Phishing Attacks Prevention and Detection Techniques

Ritika Arora, Sharad, Sanjeet Singh[1], Narendra Kumar[2] and A. K. Saini[2]
Chandigarh University,Gharuan, Punjab,India
1 darpan.anand.agra@gmail.com
2 The ICFAI University, Jaipur
aksaini@iujaipur.edu.in

Ritika Arora, Sharad, Sanjeet Singh[1], Narendra Kumar[2] and A. K. Saini[2], Phishing Attacks Prevention and Detection Techniques - Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9). ISSN 1567-214x, Keywords— Phishing attacks , Antiphish Technologies, Privacy , Security

Abstract:

Phishing attacks are online security attack which involves obtaining sensitive information. The attacker creates the precise copy of the prevailing web content to fool users so on hack their personal financial data, online banking passwords, ATM Card number. Phishing is becoming more hostile day by day and its detection is incredibly important. Phishers choose those websites which are visually and semantically just like those real websites. It affects diverse field like e-commerce, digital marketing by sending spam emails and develop identical websites which resembles original one. As a prevention method we are able to examine the properties like data set, feature extraction and detection algorithms, performance evaluation metrics using detection techniques. The main aim of our study is to propose a safer framework for detecting phishing websites with high accuracy in less time. This paper focuses on a comparative study and analysis of varied phishing detection mechanisms and several other countermeasures to beat them.

Introduction

The advent of recent communication technologies has had tremendous impact within the growth and promotion of companies spanning across many applications including online-banking, ecommerce, and in social networking. The technological advancements come in addition to new sophisticated techniques to attack and scam users All web browsers and servers take almost every care to form guarantee the safe business through internet but still they're prone to attacks like phishing that targets a user sensitive information through a phony website that appears almost like a legitimate site, or by sending a phishing email. The e-mail contains messages like ask the users to enter the private information so it's easy for hackers to hack the information[1].Website based attack continued to come up with billions of dollars in fraudulent revenue of expense of individual user and organization. The black list method is that the most typical method to detect malicious URLs by many antivirus groups. the most objective of all financial service organization is to possess safe and secure environment. Security of online banking transactions is one in all the foremost important challenges to the banking sector. Billions of monetary data transactions are conducted online a day, and bank cyber-crimes happen a day by skilled criminal hackers through manipulating the bank’s online system. Commonly spoofed website include eBay, PayPal, With the increase in phishing attack within the world, countries are now finding ways to curb it . so as to beat these, there's an urgent have to find solutions to stop phishing attacks[2]. Even a user with excellent security software can fall prey to a phishing attack, because for the most part they depend entirely on information typed into a form, not malware infection of a computer[3].Attackers are employing various technical spoofing tricks like URL manipulation, hidden elements to seem their site as similar because the target website[4] the foremost effective solution to phishing is educating users to not blindly follow links to internet sites where they're to enter personal information[5].In preparation for our own research to raised understand the user and their role falling victim to phishing attacks, we conducted systematic literature review of phishing research. The paper is split into five sections which has existing literature on the currently avail-able methods of phishing we offer the methodology and analysis of our research by outlining the protocol and to collect and analyze our data set operations.

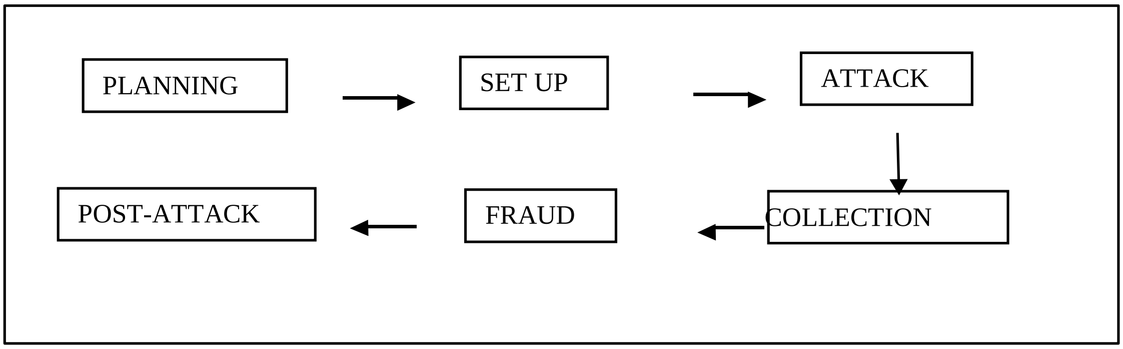


Figure1. Process of Phishing Attacks

The phishing attacks are performed within the following steps:

1. Phishers founded a duplicate of the initial website which incorporates setting up the online server afterwards applying the DNS server name, and creating the online pages just like the destination Website, etc.
2. This step includes sending great amount of spoofed e-mails to focus on users within the name of these legitimate companies and organizations and trying to convince the potential victims to go to their websites.[6]
3. When the Receivers will receive the e-mail, they'll tend to open it, and by clicking the spoofed hyperlink they're being asked to input their information within the e-mail
4. The recipient opens malicious attachment depending upon the content of email and completes a form, or will visits an internet site.[7]
5. The attacker gather the victim’s sensitive information and

will exploit it within the future.

1. Classification of PhishingAttacks

Phishing attacks can be classified into various types which are described below.

1.1 Deceptive Phishing

In this technique the phished webpage will ask the user to enter details to verify account information,, fictitious account charges, undesirable account changes, system failure requiring users to re-enter their information, new free services requiring quick action, and plenty of other exciting offers so on develop interest in users mind with the hope that the victim will click on the link as will provide the confidential personal information to the bogus webpage which might be further wont to perform scams[8].

1.2 Malware Based Phishing

This technique involves making run a malicious code on user’s machine which is capable of performing tasks which can provide details of the confidential data entered by the user. Malware may be introduced within the user’s machine as an attachment, by exploiting security vulnerabilities, as a downloadable file from an online site.[9]

1.3 WebTrojans

In this technique, the pop-up invisibly runs when users are trying to log in and that they collect the non-public information from the user’s machine locally and transmits the knowledge to the server the phisher is using to gather information of the victims.[10]

1.4 System ReconfigurationAttacks

In this technique, the phisher modifies settings on a user's PC for performing various malicious operations without the knowledge of the user. For example: URLs in a very favorites file may be altered to direct users to appear an internet site which is visually a twin of the target website. For example: a shopping website URL is also changed from "www.flipkart.com" to "www.flipkarT.com".[11]

1.5 Pharming

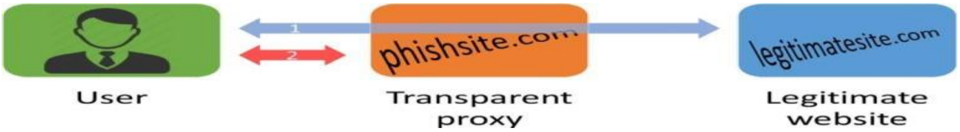
This technique modifies the company’s host file or DNS so when the user wants to log in or access that website, the changes made by the phisher will lead to opening of phished website rather than the legitimate one. Hence used will submit the knowledge to a phished page[12].

1.6 Content InjectionPhishing

In this technique, the hacker replaces some a part of code from the legitimate website which successively ends up in submitting information to the server employed by the phisher rather than submitting to the legitimate website.[13]

1.7 Man-in-the-Middle Phishing

In these attacks phisher positions, themselves between the user and also the legitimate website or system. When the user isn't active on the system then they'll sell or use the knowledge or credentials collected.[14]



1.8 C

lonePhishing

It is kind of phishing attack which have websites that are usually utilized by victims imitated by phishers. the important website is counterfeit by the clone and requests users for login information. When the user provides their login information, this offers a chance to the phisher to stay these information on his own server during a database record, after saving all the specified information, these criminals then takes the users to the authentic website. a standard example are websites that mimic companies that provide online sales like Amazon, Walmart etc.

1.9 Spear Phishing

Just as the name suggests, it's directed to a specific person or a gaggle of individuals. So, it's not like clone, where criminals cast a large net to lure anyone who visits the web site but rather emails are sent to some selected people, it can be a complete organization or institution. Usually the chosen people have a standard variable.[16]

1.10 E-mailspoofing

It is one amongst the foremost common variety of cybercrime.The user tends to lure the client during this method by giving lucrative offers and it's easier for the criminals to convince the client to click on a fraudulent file or link within the email . it's counterfeit of the e-mail header in order that the message appears to possess originated from someone or somewhere apart from actual source, example a spoofed email may pretend to be from a well-known shopping website,asking the recipient to produce sensitive data such as password or ATM-card number

2. Literature Survey

The word ‘‘phishing” was discovered during a Usenet newsgroup called AOHell on January 2, 1996, to explain the theft of users’ credentials on America Online (AOL) by a gaggle of hackers and since then, the phishing attacks are on increase with huge financial and reputational damage to online users**.**

Eduardo Benavides et al. [17] proposed the technique for prevention of Phishing Attacks. Deep Learning has emerged one amongst the foremost efficient techniques within the field of machine learning. it's implemented by neural networks and its most versatile feature is that it can increase in processing capabilities .The results are often obtained by classification of algorithm on the premise of methodology which comprises of supervised, unsupervised and hybrid. Through this method author describe the threats which occur thanks to spear phishing attacks. For future work, a comparative study is being done to see which concludes that Deep Learning algorithm is that the only in determining bogus sites. To accelerate performance within the execution of Deep Learning algorithms, design models or algorithms to combat phishing attacks, and by analyzing the similar characteristics within the URL pages generated by recurring bots.

Luca Allodiet al.[18] defined a URL based taxonomy. Various Phishing model is being implemented like Web Crawling,PhishTank during which specific set of existing feature represents a particular class within the classification models. the most aim of the author is that the author is to present a survey that investigate the pattern of URL based phishing behavior in real time environment. For achieving the results on different platforms the author has made some sample to check behavior in both online and offline mode .The use of JSON is being implemented because it is a superb sample for analyzing behavior.Another method being implemented is that the web crawler because it is developed to gather and store the knowledge within the records in an automatic way. The author has provided the decision on the relevance of the feature supported the info obtained on the dimensions weak, moderate and powerful which is on the premise of extraction qualitative and quantative measures.Results are being found on the premise of extraction method and interpretation through analysis of behavior.

Emmanuel Gbenga Dada et al. [19] has described various techniques for detection of phishing attacks. After analyzing the simplest suited method is machine learning .The author has done comparisons of strengths and downsides of the prevailing Machine learning approaches and open source problem in spam filtering .For evaluating the performance stochastic optimization techniques and evolutionary algorithm is being applied in spam filtering. the most aim is to present a framework for brand spanking new technique for linking multiple folders with an innovative filtering model. For measuring the effectiveness of any spam filter the author survey on the premise of datasets and performance metrics.

Nathezhtha.T et al.[20] emphasis various methods for efficiently detecting phishing attacks .The phishing websites are often detected with high accuracy through methods like comparison of blacklist and whitelist URL.Machine learning technique use web page Based for indentifying the phishing URL CATINA. Vaidehi.V et.al proposed approach which is solely supported the google page rank by using Page rank value. For achieving the results phishing URLs are being collected from the PhishTank .The data set is being divided into 70:30 ratio which is followed by the Heuristic Based Detection .The Experimental analysis has been done precisely to detect the phishing websites and produces detection accuracy of both phishing attack and 0 day phishing attacks.

Syed Rizvi et al.[21] has described the attacks on IOT devices through a threat model that allow to systematically analyze security solution to scale back potential risk. Mapping across various devices is being done at each zone of the model.It includes developing new risk assessment methodologies so as to tame the aspects that influence IOT and its numerous devices. The comparison is being done which offer analysis of IOT system security in respective environment. Various tools are getting used across to attain the results which incorporates network mapping tools, Packet sniffing applications. The model is essentially apt for network security professionals to approximate the danger of implementation in new IOT devices. Orunsolu et al[22] has proposed machine learning based predictive model to enhance efficiency of Anti Phishing Schemes .This model works on the strategy of feature selection method, website behavior using incremental based system.Implementation of varied anti phishing kits is being in serious trouble secure transactions.The method that is getting used is that the subject area approach that encompass the sorter module and signature detection module to gift a good weaponry for phishing kit preparation

The results area unit being analyzed on the premise of parameters like true positive rate, false positive rate and therefore the accuracy is being compared with the opposite existing

system that encompass NB and add with information sets consisting of twenty five41 ‘phishing pages and 25,000 legitimate pages.The author has discovered that new approach technique is far higher and correct as compare to existing phishing approaches.

Consistent with the experimental and comparative results from the enforced classification algorithms, Random Forest formula Adaboost, K-star, kNN (n= 3), Random Forest, SMO and Naive Thomas Bayes with solelyinformatics based mostly options offers the most effective performance with the ninety seven.98% accuracy rate for detection of phishing URLs.

The authors findings can facilitate to boost the understanding of phishing email drawback Associate in Nourishing work on developing an extension for security indicators which will check the vulnerability of the network decisions and alert the users if it will cause phishing attack before the particular call to the individual server.

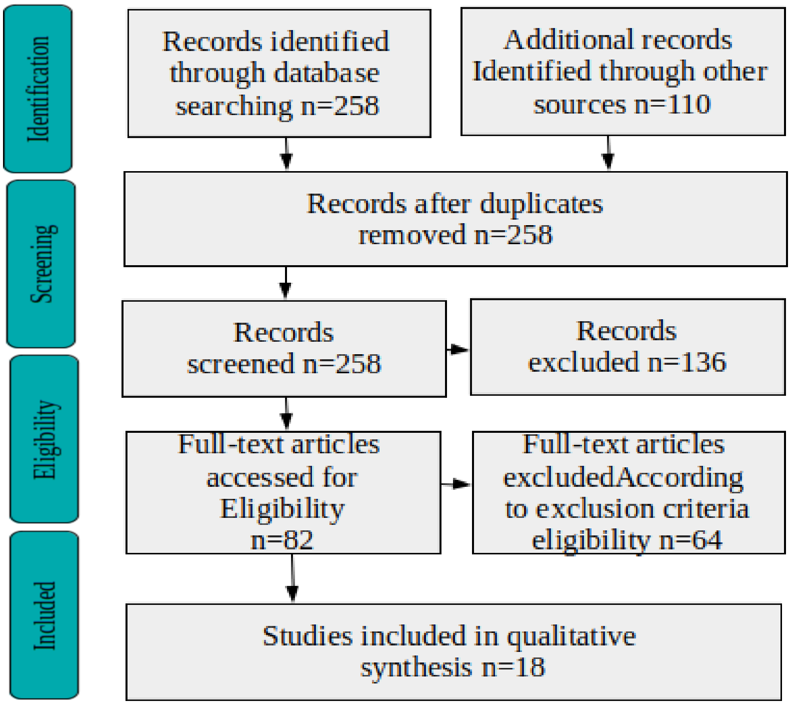

Identification
Screening
Eligibility
Included
Records identified through database searching n=258
Additional records Identified through other sources n=110
Records after duplicates removed n=258
Records screened n=258
Records excluded n=136
Full-text articles accessed for Eligibility n=82
Full-text articles excludedAccording to exclusion criteria eligibility n=64
Studies included in qualitative synthesis n=18

Figure 2. Flow diagram of evidence acquisition.

The central role played by the user in phishing attacks is that to precisely understand this state of user-centered phishing research, including a wide range of methodological approaches andpotentially significant attack attributes. On the basis of the research findings methods are being adopt which include more traditional research methods . We are also interested, however, in more additional passive methods. For instance, Alsharnouby et al. used eye tracking techniques to obtain the data about user attention to site authenticity (2015). The results which are being observed showed that the browser elements provided a positive impact to detect phishing websites, Indeed, Dhamija et al. also accentuated that visual deception can fool users.Standard security indicators are not operative enough, for their study of detecting a phishing website. These studies establish the effectiveness of human-centered research on phishing

3. METHODOLOGY USED FOR THE DETECTION OF PHISHINGATTACKS

Our systematic literature review fixated on published research on phishing. We collected our data by starting with all the research publications on phishing that are included in the Digital Library of Scopus, web of science, PubMed. We completed the data extraction and then implemented a qualitative assessment protocol that utilized exclusion and inclusion criteria to come up with a collection papers that were appropriate and relevant for our analysis. Based on the synthesis performed in the previous step, we advanced to conduct the report, and to demonstrate the information gathered by the analysis.

4.1. Technical Attributes of Phishing Attacks

Seventy out of the 81 collected papers included research that focused on the technical attributes of phishing attacks. We have distinguish these attributes into four groups, ranging from the appearance of the phishing attempt (Salem, O, Hossain et al.) such as the look of fake websites and graphical similarities, authentic websites, feature selection and extraction method such as the use of personalized data in the phishing attempt, and indicators of deception (Rao, R.et al, 2015), such as security tools indicating the authenticity of websites. Detection technique is the most common research focus throughout the papers..

Author, Year	Technique Used	Phishing Objective	Methodology Applied	Main Features

Chen, W., Zhang, W., Su, Y(2018)	Long Short Term Memory, Neural Network Recurrent	New Proposal	URL obfuscation	Phishing pages are being and the LSTM Algorithm is trained with the 12 websites. This finally produces effectiveness in the detection of new false sites.
Yi, P., Guan, Y.Zou,, (2018)	Deep Learning Algorithm	Detect Phishing attacks	Internet Protocol Flow	It focuses basically on the framework to detect phishing pages .Two types of characteristics of false sites are being classified with the original ones. Model of deep learning Algorithm is being proposed.
Pereira, M., Coleman, S., Yu, B., DeCock, M., ,(2018)	Random Forest CNN	Developing a new model	Domain generation Algorithm and fraudulent URL.	The author proposes tool known as Word Graph which generates dictionaries similar to those of DGA.
Rao, R.S., Pais, A.R. (2018)	Machine Learning	Comparative Study	Random Forest,J48,Regression, Bayes Network, AdaboostMl	To indentify the phishing websites based on the features extracted from URL website Content and third party hyperlinks.

Fatima Salahdine (2019)	Artificial Intelligence Based defense Mechanism	Analytical Study	Filtering Tools, Machine learning Tools	To identify the malicious attacks and what are the possible countermeasures to be safe Novel detection techniques should be used to obtain accurate results.
Bakhshi, T (2008)	Deep Learning Network	Behavioral Study	Sequential Minimal Optimization	This study has been included because it contains different characteristics that may be extracted from deceptive sites.
Das,S., Dingman (2018)	Machine Learning Algorithm	CNN	Euclidean Distance	This solution uses the technique applied in rendering of the images.CNN is used to detect visual similarities between the images.
R. Verma and A. Das	Feature Selection Algorithm	Visual Similarity	Malign Phishing Software	The behavior features of the images depend upon the visual similarities monitored.

4. Analysis Of The Techniques For The Detection Of PhishingAttacks

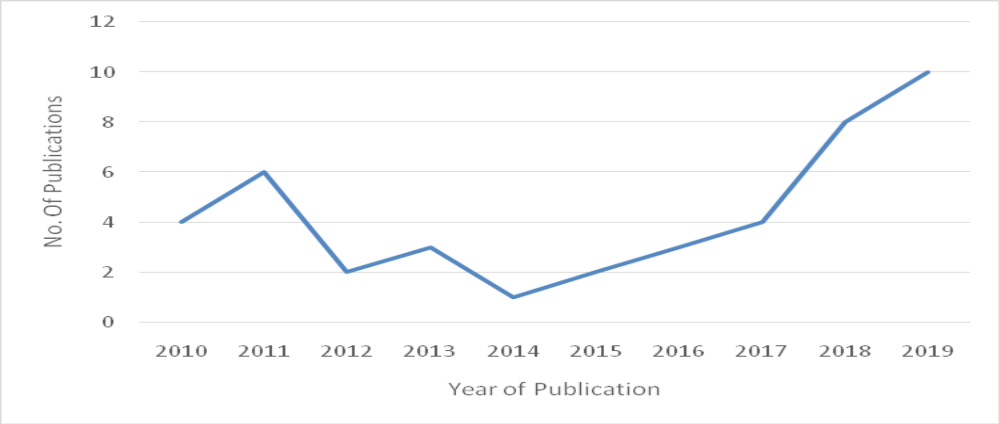
Phishing has become a severe problem in the Internet society. Researchers have developed models and guidelines for supporting online consumer trust. Existing literature deals with trustworthiness of website interface designs and policies, website content and methods to foster customer relations. The techniques are described in detail below:

S. No.	Techniques	Author	Methodology	Advantage
1.	SURF(Speed Up Robust Feature)	Herbet Bay	It is a feature detector technique used in object recognition .It is used to compare similar hyperlinks between legitimate and malicious website.	Matching Technique provides accurate results in less time
2.	SEADM (Social Engineering Attack Detection Model)	Monique Benzuidenhout	This model is based on Decision Tree.	Helps to detect using Phishtank Model
3	Anti Phishing Tool	Jordan Crain	These tools are effective in indentifying phishing websites .	Reliable means of detecting Phishing websites.

4.	Link Guard Algorithm	Raphael Olufemi Akinyede	This technique is used for analyzing difference between visual and actual link.	Used to calculate similarities of URL with a trusted site
5.	Content Filtering	Karishma Varshney	It follows Bayesian Additive Regression Tree.	Gold Phish tool implements this technique and uses Google as its search engine. This mechanism gives higher rank to well-established web sites.
6.	Honeypots	ShubikaChuahan	It follows PhishDekt Algorithm	Honeypots are deployed to collect critical information.It is based on two factor authentication method.
7.	PhiDMA Model	GunikhanSonowal	It follows String Matching Algorithm.	Based On comparison of URL

Although there are many techniques exists for detection of phishing but it is still become a thought-provoking work to notice fake web sites with the existing methodology. There are various techniques available like blacklisting, white listing, SURF, ontological Model ,heuristics and machine learning to detect phishing but machine learning is being extensively used. Sheng, S., Holbrook et.al (2018) provides Anti Phishing Simulator which aims to regulate the protection of knowledge and provide security to prevent infringements and to check whether the incoming mail has dangerous content.

Our analysis and findings reveal that the majority of the researchers noted that URLs and the appearance of spoofed websites are key indicator of phishing attempts. Thus, they anticipated new security tools, such as browser extensions and warning indicators, etc, to reduce the likelihood of users dropping victim to phishing schemes. While it is extremely significant to provide technical solutions, we believe that understanding the human factors that allow a phisher to successfully exploit the user is vital for detection, prevention, and mitigation strategies. Risk communication is an emerging field in phishing that pursues to employ more efficient training methods for just these reasons. Four of the papers studied provided game-based risk communication training as a solution to mitigate such threats, for instance. However, to develop the most effective collection of such tools and strategies, more research should focus on understanding the mental models, situational factors, and related behaviors of users.



5. DISCUSSIONS AND FINDINGS

In this graph is has been observed that throughout the course of our systematic literature review, we found specific trends in phishing research. Although the term “phishing" was coined in 1996 but the academic researchers did not begin publishing about phishing until 2004 (Dunham, 2004). The user-centered study we see in our data set is from 2010 with four papers published in this domain, we see a positive trend that ends in 2019, with ten papers published in the area.

6. CONCLUSIONS

In this paper, we have analyzed various phishing detection approach and their techniques that increases the webpage security through checking the hyperlinks in the source code of the email webpage. A review of the state of the art algorithms been applied for classification of different URLs depending upon their classification By applying these approach in future, the precision and detection rate can be measured. In general, the figure and volume of literature we reviewed shows that substantial progress have been made and will still be made in this field.

Based on our analysis of published phishing research till date, we find support for the potential importance of user studies in this field of research and for, better reporting in future studies in this field. Preventing phishing attacks is the main priority and a major challenge in the domain of secure computing. While researchers and practitioners mostly provide technical solutions to solve phishing-related issues, our examination of phishing research suggests that social resolutions, focused on users, themselves, might offer an important aspect to counter these attacks. Phishing research papers from the Science Direct Digital Library revealed that only 13.9% of relevant published papers from 2010 to 2018 included any kind of user-focused study, and these studies primarily focused on usability or testing of tools developed by the scholars rather than reconnoitering the ways different kinds of users approach and make sense of phishing attempts.

As future work, a comparative study can be done using the detecting algorithms and which is best suited for determining malicious sites. In addition, it has been planned to design models for detecting phishing attacks by analyzing the similar characteristics in the pages.

REFERENCES

[1] Gupta, B.B., Tewari, A., Jain, A.K., & Agrawal, D.P. (2016) Fighting AgainstPhishing Attacks: State of the Art and Future Challenges. The Natural Computing Applications Forum, pp1-26.

[2] Aburrous, M., Hossain, M.A., Dahal, K., Thabtah, F. (2010) "Intelligent phishingdetection system for e-banking using fuzzy data mining", Journal of Expert Systems with Applications, (In Press) DOI:10.1016/j.eswa.2010.04.044,Elsevier.

[3] Rao, R. S. & Ali, S. T. (2015) A Computer Vision Technique to Detect Phishing Attacks. s.l., Fifth International Conference on Communication Systems and NetworkTechnologies.

[4] Dhamija, R. and Tygar, J.D. (2005) The Battle Against Phishing: Dynamic SecuritySkins. Symposium on Usable

Privacy and Security (SOUPS): Pittsburgh,USA.

[5] Ye, Z., Smith, S. and Anthony, D. (2005)Trusted paths for browsers.ACM Transactionson Information and System Security, 8 (2),pp153-86.

[6] Lynch, J. (2005) Identity theft in cyberspace: crime control methods and theireffectiveness in combating phishing attacks. Berkeley Technology Law Journal,20(259).

[7] Salem, O., Hossain , A. & Kamala, M. (2010) Awareness Program and AI based Toolto Reduce Risk of Phishing Attacks. 10th IEEE International Conference on Computer and Information Technology:Bradford.

[8] Sheng, S., Holbrook, M.B., Kumaraguru, P., Cranor, L.F., and Downs, J.S. (2010)Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the CHI Conference on Human Factors in Computing Systems (Atlanta, Apr. 10–15). ACM Press, New York, pp 373–382.

[9] Rosiello, A. P. E., Kirda, E., Kruegel, C. &Ferrandi, F. (2007) ALayout-Similarity-Based Approach for Detecting Phishing Pages. Security and Privacy in Communications Networks and the Workshops,pp454-463

[10] Vr
banˇciˇc, G., Fister, I., Podgorelec, V.: Swarm Intelligence Approaches forParameter Setting of Deep Learning Neural Network. In Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics—WIMS ’18, pp. 1–8(2018)

[11] Ra
o, R.S., Pais, A.R.: Detection of phishing websites using an efficientfeature-based machine learning framework. Neural Comput. Appl., 1–23 (2018)

[12] Sur
, C.: DeepSeq: learning browsing log data based personalized securityvulnerabilities and counter intelligent measures. J. Ambient Intell. Humaniz. Comput., 1–

30(2018)

[13] Basnet, R., Mukkamala, S., Sung, A.H.: Detection of Phishing Attacks: A Machine Learn-ing Approach. In Soft Computing Applications in Industry, pp. 373–383.Berlin, Heidelberg, Springer Berlin Heidelberg(2008)

[14] Chen, W., Zhang, W., Su, Y.: Phishing Detection Research Based on LSTMRecurrent Neural Network, pp. 638–645. Springer, Singapore(2018)

[15] Zhang, J., Li, X.: Phishing Detection Method Based on Borderline-Smote DeepBelief Network, 45–53. Springer, Cham(2017)

[16] Zhao, J., Wang, N., Ma, Q., Cheng, Z.: Classifying Malicious URLs UsingGated Recurrent Neural Networks, pp. 385–394. Springer, Cham(2019)

[17] Eduardo Benavides, Walter Fuertes, Sandra Sanchez and Manuel Sanchez (2019) Classification of Phishing attack solution by employing deep learning Techniques:A systematic Literature Review Science Direct52-58

[18] Luca Allodi,TzoulianoChotza,EkaterinaPanina,Nicola Zannone(2019) On the new need of new spear Phishing attacks,Article in IEEE Security and PrivacyMagazine.pp2-10

[19] Emmanuel Gbenga Dada, Joseph Stephen Bassi, Haruna Chiroma (2019) Machine learning for email spam filtering:review,overview and open search problem Elsevier.

[20] Nathezhtha.T, Sangeetha.D,Vaidehi.V(2019) WC-PAD: Web Crawling basedPhishing Attack Detection.

[21] Syed Rizvi RJ Orr[a],Austin

Cox[a],PrithveeAshokkumar,Mohammad R.Rizvi(2019) Identifying the attack surface for IoT network 1

[22] A.A. Orunsolu , A.S. Sodiya , A.T. Akinwale A predictive model for phishing detection(2019) Journal of King Saud University –Computer and Information Sciences pp 1-16

[23] Routhu Srinivasa Rao , Tatti Vaishnavi,, Alwyn Roshan Pais (2019) PhishDump: A multi-model ensemble based technique the detection of phishing sites in mobiledevices Pervasive and Mobile Computing 60-70.

[24] OzgurKoraySahingoz,Ebubekir Buber,Onder Demir,Banu Dir(2019)Machine learning based phishing detection from URLs Expert Systems With Applications pp8-18.

[25] Bakhshi, T., Papadaki, M. and Furnell, S. (2008), “A Practical Assessment of Social Engineering Vulnerabilities”, Proceedings of the 2ndInternational Conference on Human Aspects of Information Security and Assurancepp12-23

[26] Das, S., Dingman, A., and Camp, L.J. (2018), “Why Johnny Doesn’t Use TwoFactor: A Two-Phase Usability Study of the FIDO U2F Security Key”, 2018 International Conference on Financial Cryptography and Data Security(FC).

[27] R. Verma and A. Das, “What’s in a URL: Fast Feature Extraction and Malicious URL Detection,” Proc. 3rd ACM on International Work-shop on Security and PrivacyAnalytics (IWSPA ’17), The Scotts-dale, Arizona, USA, pp.55–63, March2017

[28] Alsharnouby, M., Alaca, F. and Chiasson, S. (2015), “Why phishing still works:User strategies for combating phishing attacks”, InternationalJournal of Human-Computer Studies, Vol. 82, pp 69-82.