Journal of Theoretical and Applied Information Technology
31st December 2014. Vol.70 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CURRENT STATE OF ANTI-PHISHING APPROACHES AND REVEALING COMPETENCIES

[1] HIBA ZUHAIR ZEYDAN, [2]ALI SELAMAT, MAZLEENA SALLEH
[1] Faculty of Computing, Universiti Teknologi Malaysia,
81310 UTM Skudai, Johor, Malaysia.

ABSTRACT

Phishing has become a substantial threat for internet users and a major cause of financial losses. In these attacks the cybercriminals carry out user credential information and users can fall victim. The current solution against phishing attacks are not sufficient to detect and work against novel phishes. This paper presents a systematic review of the previous and current research waves done on Internet phishing mitigation in different areas of expertise and highlighted phishing attacks types and some existing anti-phishing approaches. Further the discussion about novel phishes and identify the elements of issues highlighted. The review can be valuable source of information to find and identify recent gap and challenges to fulfill the security flaws.

Keywords: *Anti-phishing, detection, novel, credentials, client*

1. INTRODUCTION

The internet phishing is a new type of cyber-crime and type of online identity theft. The basic aim of phishing attacks is to steal personal credentials from users such as online banking user id and password and credit card data [1]. The electronic commerce organizations have been faced and loose their reputation because of these phishing tricks. The attackers use a combination of technical and engineering spoofing techniques and make a financial profit. In these techniques the attacker use legitimate-looking but fake emails and use fake websites for steal important information. There are many types of anti-phishing solutions proposed to tackle these tricks and attacks but still the users personal information and security are on risk. One of the main reason is rapidly growth and advancement of phishing tricks noticed. These tricks bypass the existing solutions and users lose their credentials information [2]. According to international non-profit organization APWG (Anti-phishing work group) that the volumes of phishing websites have been rapidly increases since 2010. In another report it mentioned that these attacks targeting different organizations and industries such as banks, online payment services, retail and ISP services, etc. [3, 4]. According to author in 2012 the internet users lost 687 million dollars because of phishing attacks and it was 30% more compare with 2011 attacks [5, 6]. The existing solutions are not sufficient and effective against novel phishes. We discuss these issues in this review and discuss some most popular anti-phishing proposed solutions. Further, review provides a suitable scenario for anti-phishing solutions with clear characterization and detection capability against novel phishes. This review will help to find and identify recent gap and challenges to fulfill the security flaws to new researchers for develop anti-phishing solutions. The paper shows a systematic review of existing research on Internet phishing mitigation. The main purpose is to show the advance in the wave of research, motives, mitigation achievements and proposal strategies with their relative merits. Moreover, it identifies the least focused domains of research, barriers on their solutions as long as the expanding scope of the problems which still need further efforts in the future.

The paper is structured as follows: The section 2 presents a brief research philosophy and main contribution. The section 3 presents the anti-phishing techniques and its applications. The section 4 defines about anti-phishing solutions in terms of detection capability and brief comparison. The section 5 elaborates the difference of anti-phishing and novel phishes in detail. The last section 6 is related with future prospective and conclusion of the review.

Journal of Theoretical and Applied Information Technology
31st December 2014. Vol.70 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. RESEARCH CONTRIBUTION AND PHILOSOPHY

This section describes the existing anti-phishing solutions in term of detection capability against novel phishing through systematic review. The systematic literature review is basically used to investigate the most important aspects of the former researches done on a specific subject. It extracts and maps out useful information by using an effective research framework and significant statistics. All this can be done through several steps: formulating research questions, search and selection processes, application of certain feasible criteria with categorization schemes; and then presenting the answers of research questions on tables and statistics [7-9]. Figure 1 clearly illustrates the conceptual framework of systematic review which is presented in [9]. It contributes an inclusive taxonomy, which is divided into three categories shows in Figure 1. In the first level the anti-phishing solutions are classifies on the base of detective approaches and application level. The second level identifies the new variants of phishes and reaction of existing solutions. The last level defines the next wave for further research work.

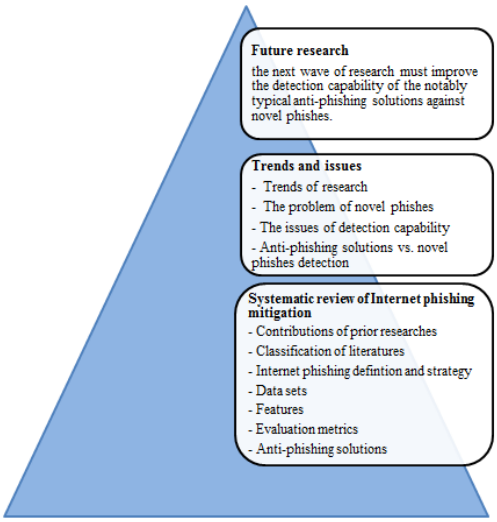

Figure 1: Inclusive taxonomy [9]

Figure 2, illustrates the response of systematic literature review via the following processes:

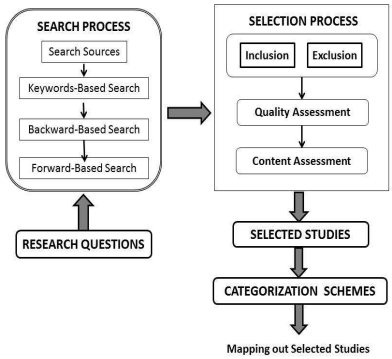

Figure 2: Framework of systematic review

2.1 The Search process

In this process retrieve the previous studies and publications, an exploratory search is done. It is implemented by using some publically available digital libraries such as IEE Explore, Science Direct, Scopus, Google Scholar, ACM, Springer Link, and Emerald. The set of the retrieved studies includes journals and international conference papers, book chapters, magazines and theses ranging from 2008 to 2014. For the purpose of search, some keywords such as internet phishing, phishing detection, anti-phishing, phishing prevention, and phishing mitigation, etc. are used. Furthermore, an advanced search based on article titles, authors and journal titles is achieved. Keywords were used individually or collectively with the help of some operators. To retrieve references corresponding to or cited from the initial set of retrieved publications, two dimensional searching is done: backward and forward search. Finally, the set of retrieved publications totally results in 197 publications to be refined in the selection process.

2.2 Selection process

This process actually narrows down the set of the retrieved publications to a set of more extensive and more relevant publications on internet phishing mitigation. By this way, the outdated and out of place publications contained in the original set are removed by inclusion and exclusion criteria. These criteria involve including the higher ranking sources and excluding the outdated and irrelevant studies in terms of quality assessment and data synthesis as presented.

2.3 Categorization schemes

There are many categorization schemes used for mapping out the selected publications in the form of statistics according to the type of research

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and contributions. These schemes were adopted by authors in [9]. For the purpose of responding to formulated research questions. Thus, this review utilizes these schemes to categorize the selected publications into certain dimensions. After selection the systematic review comes with specific related studies, which are presented in below sections.

3. ANTI-PHISHING APPROACHES AND APPLICATIONS

The anti-phishing solutions are based on its applications and approaches level. In anti-phishing literature the most of existing approaches are based on detection techniques. These approaches are categorized into different types such as some are based on lists, hybrid, and information flow [10-12]. In list type approaches contains blacklists ad whitelists approaches and rely on regularly updated lists of well-known phishing and legitimate URLS. These are widely used and achieve high detection accuracy with low false positive rates. However these approaches are cannot detect and identify fresh phishes because of lists, where maintenance and human resources required and the scalability and run time are not suitable. This is the reason the list based approaches combine with other approaches [2, 3, 10, 12-20]. The Heuristics based approaches are predicted through one or more websites features like URL, source code and visual features. These two types list and heuristic approaches can work against fresh phishes and produce low detection accuracy [10, 15, 21, 22]Because of these reasons the researchers proposed hybrid approaches. These hybrid approaches are combination of one or more approaches to work against these limitations. The hybrid approaches are more effective and they can avoided via novel phishes for instant vulnerabilities of web applications to insert malicious codes [2, 10, 22]. Another type is flow based solutions and relies on attaching some random credential before and after user credentials to a phishing website. This is the main reason the phishers cannot identify real credentials. However these approaches are fail when phishing websites allow limited number of random credentials to be submitted [2, 10, 12, 22].

The application level approaches have been roughly categorize into client side, server side and client and server level [3, 21] illustrates in Table 1. According to table the direct interaction of internet users through web browser is potentially on risk. That's why most of approaches are on client side level in the shape of tools in popular browsers such as Mozilla Firefox, Internet Explorer and Google Chrome, etc. These integrated tools keep user activities and track during web browsing and inform them in time about phishing websites. These approaches are suffered from some short comes like design of intuitive interface, correct warnings, help system and detection accuracy [23, 24]. The existing client side approaches are deployed for active notification and risk of interrupt browsing process. These notifications are not acceptable in the case of misclassifying legitimate websites as phishing websites, which may decrease user trust and reliability on anti-phishing tools and on web browser [4, 25]. Although server side solutions are effective but there is another problem in server-side anti-phishing solutions and that is not effective against web banners and fail when users rarely notice the absence and existence of these indications [21]. The most of commercial organizations are using client-server structured applications such as Netcraft, Google, and Microsoft. But in client-server structured applications are frequently request for update and need maintenance from database server. When phishing website is encountered that time the Netcraft toolbar contacts Netcraft's server for online database verification [26].

4. ANTI-PHISHING SOLUTIONS

In this section we discuss the notable anti-phishing solution. The most of the anti-phishing have been proposed and implemented in the form of anti-virus software, web browser plug-in, add-on's, extensions ,toolbars and are browser independent as shows in table 1. Further these solutions rely on different application levels and exploit different approaches like white lists of known legitimate URLs, black lists, white lists, heuristic and hybrid and information flow approaches to combat either phishing web sites or phishing emails. The B-APT proposed and developed for US financial institutions as a list based anti-phishing solution. It was designed for identifying websites through Bayesain filter and based on tokens that are extracted by document object model DOM analyzer [27]. Another approach proposed [28] AIWL (automated individual white list to protect user online credentials. Whitetaker, Ryner and Nazif proposed and upgraded Google phishing blacklist with a classifier toolbar to identify phishing websites because of some typical characteristics. Another author enhanced a blacklist of PhishNet by

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

generating new URLs using heuristics and checking if they resolved by DNS lookup.

There is another example of heuristics based anti-phishing solution SpoofGuard [29] developed in Stanford University as a browser plug-in to identify phishing websites based on a set of heuristics. Therefore some other researchers proposed PILFER as an email filter and based on ten different heuristics and publically available for legitimate and phishing e-mails. Some other academic researchers in Carnegie Mellon University proposed [29] CANTINA (content based anti-phishing) solution and based on frequency-inverse document frequency (tf-idf) algorithm to extract and retrieve tokens, meta keywords and description tags from web page source code with the help of search engine and identifying the top ranking keywords as a phishing webpage. After this another author [12] used set of filters and weighted rules to classify phishing emails in PhishCatch anti-phishing email client side plug-in. After this another PhishShark [30] developed and based on twenty heuristics for phishing websites detection.

Than CANTINA+ proposed [31] as a hybrid anti-phishing solution and upgraded version of CANTENA with new ten additional features. The four features are from CANTENA and other are novel extended features. The PhishBlock prposed [32] as an efficient hybrid system and relied on lookup and a support vector machine classifier and check the features, which are derived from websites URL, text and linkage. Some other researchers proposed information flow-based anti-phishing solutions such as Krida and Kruegel plug-in designed for observe the password field of HTML from the domain site and visited by the user [22, 33]. Another information-flow based anti-phishing tool PhishGuard used to submit bogus credentials when user login and sent original credentials to identify phishing websites. The Bogus Bitter [34] used to submitted a great number of bogus credentials with actual credentials to nullify a phishing attack. The phish tester proposed [35, 36] to mitigated phishes and exploits cross site scripting (XSS) we-browsers and some vulnerabilities to distribute malicious codes . Another RwdHash released [22, 37] to convert transparently user password into domain specific password through sending a one way hash of password and domain name.

Further many anti-phishing solutions proposed for industries products such as Firfox2, Netcraft, Microsoft phishing Filter, etc. The Netcraft produced by netcraft.com in 2010, where accesses the phishing sites through the domain registered time of visited website and also based on company maintained database [5, 38]. The Microsoft Phishing filter is an add-on and scans visited websites and warn user about potentially suspicious with the help of dynamically updated online information service run by Microsoft and then block the visited website if it is phishing. The Firefox2 offered as an anti-phishing by Mozilla Firefox and based on knows lists of malicious and phishing websites with the help of Google browsing protocol. McAfee site advisor is another database anti-phishing tool contains automated crawlers that browse websites and perform test for authenticity rating of the visited websites [38].

5. ANTI-PHISHING VS. NOVEL PHISHES

The most of existing studies addresses the issues of detection accuracy, overall effectiveness and computational cost of anti-phishing solutions toward finding an optimum anti-phishing solution. These solutions neglected the detection in term of features, URL mechanism and webpage content analysis [6, 11, 23, 35]. In this section we discuss some of these issues of anti-phishing which are rarely discussed before.

5.1 Novel Phishes

The novel phishing are based on cross site scripting and XSS, embedded object based and non-English language based websites. These types of phishes have been rapidly increased between 2010 to 2013 [12, 35]. These types of novel phishing features probably exploit web sites and its content as shows in Figure 2.

The graph shows that XSS-based phishing websites developed by phishers who exploit cross cite scripting and vulnerabilities on web browsers and obfuscate client-side scripts of the website source files to install spyware and malware into client computer. Furthermore, phishers imitate embedded objects like Flash objects, ActiveX objects, Applets on the source code file of a legitimate webpage. These exploits some URL features of webpages, which are hosted in some languages and these languages are not identified to bypass existing ant-phishing solutions. This is a gap in phishing mitigation because the existing anti-phishing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

solutions are incompetent in these phishes [12, 20, 35, 39, 40].

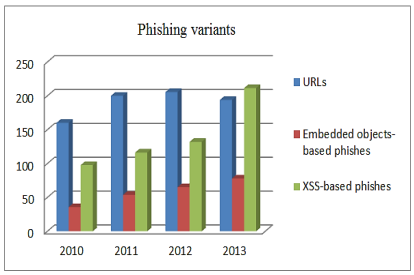

Figure 2: Phishing Variants

5.2 Detection Capability

There are many limitations present in anti-phishing solutions because of these detection capabilities against novel phishes as XSS-based phished, embedded object-based phishes, etc. [11, 12, 41]. The Table 3 shows the comparison of anti-phishing solutions against novel phishes.

Table 1: Comparison Of Anti-Phishing Solutions Against Novel Phishes

Related Work	XSS-based phishes	Embedded objects-based phishes	Language independent
Han et al. [2]	✓	×	✓
Prakash et al.[40]	×	×	✓
Xiang et al. [42]	×	×	×
Prevost et al. [43]	×	×	×
Joshi et al. [28]	✓	×	✓
Yue and Wang [30]	×	×	✓
Shahriar and Zulkernine [32, 44]	✓	×	✓
Fahmy et al. [45]	×	×	×
Whittaker et al. [46]	×	×	×
Andrě et al. [47]	×	×	×
McAfee Site Advisor [38, 48]	✓	×	✓
Likarish et al.[49]	×	×	✓

The above comparison table shows that all anti-phishing solutions have some limitations in different capabilities. The list based anti-phishing solutions are relied on automated individual white list of URLs for protecting users from online credentials, images, scripts, XSS vulnerabilities, Active X objects in webpage source code for imitation and obfuscation [2]. The most of heuristics based solutions rarely leverage novel phishing websites basically these are made with own adapted heuristics. Further these are rely on frequency-inverse document frequency (tf-idf) features and on language dependent feature based text categorization [2, 10, 20, 40, 45]. The different authors proposed solutions which are based on these types [1, 12, 28-30, 50].

The hybrid based anti-phishing solutions are efficient compare to list and heuristics based solutions due to its classifiers and they are scarcely tolerate with non-English language based phishes [2, 10, 20, 40, 45]. Furthermore, the limitation of number adapting exist to detect webpage hosted in non-English language due to its language dependent hybrid features and text-based tf-idf algorithm, which are not suitable for detection [31]. The CANTINA+ is a most effective anti-phishing solution working against zero-hour phishing websites but still have some potential incapability in non-English based phishing websites. On the other hand another information flow based solution proposed and can effectively detect most zero hour and language-hosted phishing websites because they keep the user credentials during transaction. However they can bypassed through novel phishes like in [12, 24, 30, 35].

6. LIMITATIONS OF STUDY

The set of hybrid features extracted from three parts of website; namely, HTML source code, JavaScript code and the URL in which the webpage is hosted. Detect a subset of novel phishes, i.e., XSS-based phishes, embedded objects-based phishes and phishes exploit websites hosting in any language. Include legitimate websites, phishing websites, and suspected websites in the collected dataset as well as offline and online samples. Collect the dataset from specific sources such as datasets used by current researches and well known archives of the most popular organizations concerning on Internet phishing mitigation. For example, Google Whitelist, Alexa's top sites, PhishTank and CastleCops. The cross validation of the proposed model relies on random-based evaluation, which evaluates the overall performance of this model using randomly selected phishing and legitimate websites under an environmental setup and real time conditions. The expected findings of this study may reflect some practical impacts of the adopted features on the overall detection efficacy due to the computational cost and time. It is not

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

easy to provide empirical evidence that constructed phish detection model could be considered as the optimum anti-phishing solution but at least this effort is worthwhile towards generalizing well novel phishes detection and reducing missing ones. Analysis and investigation have been made regarding to the actually used phishing and legitimate datasets, features selection criteria and evaluation metrics due to the lack of benchmark test bed in realism. Thus, to observe a clear picture to the revealed detection results, this proposed approach will be compared to the former ones. This study employs actual datasets that observed during a distinct period of time due to the short life span of phishing websites which varies from 3 minutes to 48 hours.

7. OPEN RESEARCH ISSUES

The academic and industry researchers have generally conducted their investigations in technical and sociological perspectives towards detecting phishing emails and websites [4, 38]. Researchers introduced numerous anti-phishing solutions against phish websites. Such solutions involved with various detection approaches such as blacklist and whitelist, heuristics, hybrid and information flow -based approaches [2, 3, 10, 23, 26, 39, 47]. Based on the literature, hybrid based anti-phishing solutions outperformed the other solutions due to the use of various hybrid features and classifiers. However, they are still misclassify some kinds of novel phishes that have exploit more sophisticated deceptions and advanced trickery to bypass existing anti-phishing solutions [21, 31, 32, 35, 40, 44, 46, 51]. Novel phishes like cross site scripting based (XSS-based), embedded objects-based and phishes exploit cross site scripting vulnerabilities on web browsers and obfuscated scripts to hide and distribute spyware and malware into the client's computer. Furthermore, they modify and imitate some components in the webpage's source code to redirect users to fake websites by using external links [42, 43, 45, 52, 53]. Particularly, a limited number of phish detection models have been proposed in the literature to detect the continuously evolving phish variants. And researchers have conducted their investigations to explore a variety of features for phishing detection but they have rarely provided effective set of hybrid features that can be considered as phish pattern (often named as phish profile) [13, 54-56]. Furthermore, distinct feature selection mechanisms which can be used to obtain valuable hybrid features and best features set quality is sparingly found in the literature [13, 56-60].These issues are laid behind the problem of missing novel phishes, wrong alarms, inaccurate detection and poor adaptability to novel phishes.

8. DISCUSSION AND FUTURE DIRECTION

Recently the anti-phishing solutions capability is a great challenge against novel phishes websites. More importantly these solutions analyze phishing attacks by using design features and mechanisms because of this they cannot leverage and efficient. They have lack of webpage URL and content analysis for webpage design in embedded objects like images, applets, ActiveX, etc. Furthermore the issue of leveraging obfuscated client side scripts and not probably injected by malware delivery [20, 40]. Some solutions are came with frequency-inverse document frequency (tf-idf) features, and text categorization but these are only good for specific languages [20, 61]. Another issue is that the data set used by some typical anti-phishing solutions and limited for specific languages like English. So that phishers can defeat some anti-phishing solutions by phish websites hosted in some other languages like Arabic and Chinese. The security and prevent from phishes attacks are necessary in development and growth in different fields such as financial banks, industries, transportation, and new technologies, etc. [62-64]. As a result the main challenge of new researchers is to conduct investigations toward finding an optimum anti-phishing solution in terms of detection capability against novel phishes along with efficacy factors for wider-scale detection of existing ant-phishing solutions. For future our suggestion is that an optimum anti-phishing solution, which is based on a combination of anti-phishing approaches require.

9. CONCLUSION

The existing anti-phishing solutions not work efficiently against phishes because of its continuing growth and day by day new tricks. There is a need of rich literature via wider objective, theoretical and practical contributions are needed to meet cyber security requirement and financial indexes. There is a need to consider new scenarios to test and deal with novel phishes. This will help the researcher to stimulating and enhance their interests and attention into the challenges of detection against novel phishes. This survey is most up to date and based on large material. In addition it attempts the recent

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

gap of anti-phishing campaign and makes a bridge to describe and characterize its elements. Through this survey we reveal that the issues are fall into many facts such as features and mechanism and developed for wider and effective detection of novel phishes. There is still a big gap towards finding an optimum anti-phishing solution against phishes.

REFRENCES:

[1] E. H. Chang, K. L. Chiew, S. N. Sze, and W. K. Tiong, "Phishing Detection via Identification of Website Identity," in *IT Convergence and Security (ICITCS), 2013 International Conference on*, 2013, pp. 1-4.

[2] W. Han, Y. Cao, E. Bertino, and J. Yong, "Using automated individual white-list to protect web digital identities," *Expert Systems with Applications,* vol. 39, pp. 11861-11869, 2012.

[3] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: a literature survey," *Communications Surveys & Tutorials, IEEE,* vol. 15, pp. 2091-2121, 2013.

[4] W. Kim, O.-R. Jeong, C. Kim, and J. So, "The dark side of the Internet: Attacks, costs and responses," *Information Systems,* vol. 36, pp. 675-705, 2011.

[5] G. S. Bindra, "Efficacy of Anti-phishing Measures and Strategies-A research Analysis,," *World Academy of Science, Engineering and Technology* vol. 70, 2010.

[6] P. Soni, S. Firake, and B. Meshram, "A phishing analysis of web based systems," in *Proceedings of the 2011 International Conference on Communication, Computing & Security*, 2011, pp. 527-530.

[7] H. P. Breivold, I. Crnkovic, and M. Larsson, "A systematic review of software architecture evolution research," *Information and Software Technology,* vol. 54, pp. 16-40, 2012.

[8] W. Bandara, S. Miskon, and E. Fielt, "A systematic, tool-supported method for conducting literature reviews in information systems," 2011.

[9] A. Mehmood and D. N. Jawawi, "Aspect-oriented model-driven code generation: A systematic mapping study," *Information and Software Technology,* vol. 55, pp. 395-411, 2013.

[10] M. Rajalingam, S. A. Alomari, and P. Sumari, "Prevention of Phishing Attacks Based on Discriminative Key Point Features of WebPages," *International Journal of Computer Science and Security (IJCSS),* vol. 6, p. 1, 2012.

[11] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, "An empirical analysis of phishing blacklists," in *Sixth Conference on Email and Anti-Spam (CEAS)*, 2009.

[12] W. D. Yu, S. Nargundkar, and N. Tiruthani, "Phishcatch-a phishing detection tool," in *Computer Software and Applications Conference, 2009. COMPSAC'09. 33rd Annual IEEE International*, 2009, pp. 451-456.

[13] L. Ma, B. Ofoghi, P. Watters, and S. Brown, "Detecting phishing emails using hybrid features," in *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on*, 2009, pp. 493-497.

[14] A. Upadhyaya, "Design & development of a plug-in for a browser against phishing attacks," *International Journal of Emerging Technology & Advanced Engineering,* vol. 2, 2012.

[15] B. Wardman, "A series of methods for the systematic reduction of phishing," University of Alabama at Birmingham, 2011.

[16] I. Jo, E. Jung, and H. Y. Yeom, "Interactive Website Filter for Safe Web Browsing," *Journal of Information Science and Engineering,* vol. 29, pp. 115-131, 2013.

[17] M. Bhati and R. Khan, "Prevention Approach of Phishing on Different Websites," *International Journal of Engineering and Technology,* vol. 2, 2012.

[18] W. Chu, B. B. Zhu, F. Xue, X. Guan, and Z. Cai, "Protect sensitive sites from phishing attacks using features extractable from inaccessible phishing URLs," in *Communications (ICC), 2013 IEEE International Conference on*, 2013, pp. 1990-1994.

[19] R. Dhanalakshmi, C. Prabhu, and C. Chellapan, "Detection of phishing websites and secure transactions," *International Journal Communication & Networking Security (IJCNS),* vol. 1, 2011.

[20] W. Zhuang, Q. Jiang, and T. Xiong, "An intelligent anti-phishing strategy model for phishing website detection," in *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*, 2012, pp. 51-56.

[21] S. Chaudhary, "Recognition of phishing attacks utilizing anomalies in phishing websites," 2012.

[22] H. Huang, S. Zhong, and J. Tan, "Browser-side countermeasures for deceptive phishing

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attack," in *Information Assurance and Security, 2009. IAS'09. Fifth International Conference on*, 2009, pp. 352-355.

[23] S. Purkait, "Phishing counter measures and their effectiveness–literature review," *Information Management & Computer Security,* vol. 20, pp. 382-420, 2012.

[24] A. Almomani, B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," *Communications Surveys & Tutorials, IEEE,* vol. 15, pp. 2070-2090, 2013.

[25] A. Jain and V. Richariya, "Implementing a web browser with phishing detection techniques," *arXiv preprint arXiv:1110.0360,* 2011.

[26] Y. Li, R. Xiao, J. Feng, and L. Zhao, "A semi-supervised learning approach for detection of phishing webpages," *Optik-International Journal for Light and Electron Optics,* vol. 124, pp. 6027-6033, 2013.

[27] P. Likarish, E. Jung, D. Dunbar, T. E. Hansen, and J. P. Hourcade, "B-apt: Bayesian anti-phishing toolbar," in *Communications, 2008. ICC'08. IEEE International Conference on*, 2008, pp. 1745-1749.

[28] C. Whittaker, B. Ryner, and M. Nazif, "Large-Scale Automatic Classification of Phishing Pages," in *NDSS*, 2010.

[29] N. Chou, R. Ledesma, Y. Teraguchi, and J. C. Mitchell, "Client-Side Defense Against Web-Based Identity Theft," in *NDSS*, 2004.

[30] S. Gastellier-Prevost, G. G. Granadillo, and M. Laurent, "Decisive heuristics to differentiate legitimate from phishing sites," in *Network and Information Systems Security (SAR-SSI), 2011 Conference on*, 2011, pp. 1-9.

[31] G. Xiang, J. Hong, C. P. Rose, and L. Cranor, "CANTINA+: a feature-rich machine learning framework for detecting phishing web sites," *ACM Transactions on Information and System Security (TISSEC),* vol. 14, p. 21, 2011.

[32] H. M. Fahmy and S. A. Ghoneim, "PhishBlock: A hybrid anti-phishing tool," in *Communications, Computing and Control Applications (CCCA), 2011 International Conference on*, 2011, pp. 1-5.

[33] E. Kirda and C. Kruegel, "Protecting users against phishing attacks with antiphish," in *Computer Software and Applications Conference, 2005. COMPSAC 2005. 29th Annual International*, 2005, pp. 517-524.

[34] D. Miyamoto, T. Miyachi, Y. Taenaka, and H. Hazeyama, "PhishCage: reproduction of fraudulent websites in the emulated internet," in *Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques*, 2013, pp. 242-247.

[35] H. Shahriar and M. Zulkernine, "Trustworthiness testing of phishing websites: A behavior model-based approach," *Future Generation Computer Systems,* vol. 28, pp. 1258-1271, 2012.

[36] H. Shahriar and M. Zulkernine, "Information source-based classification of automatic phishing website detectors," in *Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on*, 2011, pp. 190-195.

[37] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, "Stronger Password Authentication Using Browser Extensions," in *Usenix security*, 2005, pp. 17-32.

[38] H. Wang, B. Zhu, and C. WANG, "A Method of Detecting Phishing Web Pages Based on Feature Vectors Matching," *Journal of Information and Computational Systems,* vol. 9, pp. 4229-4235, 2012.

[39] V. Shreeram, M. Suban, P. Shanthi, and K. Manjula, "Anti-phishing detection of phishing attacks using genetic algorithm," in *Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on*, 2010, pp. 447-450.

[40] G. Ramesh, I. Krishnamurthi, and K. Kumar, "An efficacious method for detecting phishing webpages through target domain identification," *Decision Support Systems,* vol. 61, pp. 12-22, 2014.

[41] M.-E. Maurer and L. Höfer, "Sophisticated phishers make more spelling mistakes: using URL similarity against phishing," in *Cyberspace Safety and Security*, ed: Springer, 2012, pp. 414-426.

[42] R. B. Basnet and A. H. Sung, "Mining Web to Detect Phishing URLs," in *Machine Learning and Applications (ICMLA), 2012 11th International Conference on*, 2012, pp. 568-573.

[43] R. B. Basnet, A. H. Sung, and Q. Liu, "Rule-based phishing attack detection," in *International Conference on Security and Management (SAM 2011), Las Vegas, NV*, 2011.

[44] P. Prakash, M. Kumar, R. R. Kompella, and M. Gupta, "Phishnet: predictive blacklisting to detect phishing attacks," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1-5.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[45] L. A. T. Nguyen, B. L. To, H. K. Nguyen, and M. H. Nguyen, "Detecting phishing web sites: A heuristic URL-based approach," in *Advanced Technologies for Communications (ATC), 2013 International Conference on*, 2013, pp. 597-602.

[46] J. Zhang and Y. Wang, "A real-time automatic detection of phishing URLs," in *Computer Science and Network Technology (ICCSNT), 2012 2nd International Conference on*, 2012, pp. 1212-1216.

[47] H. al-Khateeb, "Security and usability in click-based authentication systems," 2011.

[48] H. Shahriar and M. Zulkernine, "PhishTester: automatic testing of phishing attacks," in *Secure Software Integration and Reliability Improvement (SSIRI), 2010 Fourth International Conference on*, 2010, pp. 198-207.

[49] A. M. Tonge and S. R. Chaudhari, "Phishing Susceptibility and Anti-Phishing Security Strategies-Literature Review."

[50] Y. Zhang, J. I. Hong, and L. F. Cranor, "Cantina: a content-based approach to detecting phishing web sites," in *Proceedings of the 16th international conference on World Wide Web*, 2007, pp. 639-648.

[51] O. A. B. Mona Ghotaish Alkhozae, "Phishing websites detection based on phishing characteristics in the webpage source code," *International Journal of Information and Communication Technology Research.*, 2011.

[52] A. San Martino and X. Perramon, "Phishing Secrets: History, Effects, Countermeasures," *IJ Network Security,* vol. 11, pp. 163-171, 2010.

[53] R. Gowtham and I. Krishnamurthi, "A comprehensive and efficacious architecture for detecting phishing webpages," *Computers & Security,* vol. 40, pp. 23-37, 2014.

[54] R. M. Mohammad, F. Thabtah, and L. McCluskey, "An assessment of features related to phishing websites using an automated technique," in *Internet Technology And Secured Transactions, 2012 International Conference for*, 2012, pp. 492-497.

[55] M. Khonji, A. Jones, and Y. Iraqi, "A study of feature subset evaluators and feature subset searching methods for phishing classification," in *Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference*, 2011, pp. 135-144.

[56] C. K. Olivo, A. O. Santin, and L. S. Oliveira, "Obtaining the threat model for e-mail phishing," *Applied Soft Computing,* 2011.

[57] F. Toolan and J. Carthy, "Feature selection for Spam and Phishing detection," in *eCrime Researchers Summit (eCrime), 2010*, 2010, pp. 1-12.

[58] I. R. A. Hamid and J. Abawajy, "Hybrid feature selection for phishing email detection," in *Algorithms and Architectures for Parallel Processing*, ed: Springer, 2011, pp. 266-275.

[59] H. Peng, F. Long, and C. Ding, "Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 27, pp. 1226-1238, 2005.

[60] R. B. Basnet, A. H. Sung, and Q. Liu, "Feature selection for improved phishing detection," in *Advanced Research in Applied Artificial Intelligence*, ed: Springer, 2012, pp. 252-261.

[61] G.-G. Geng, L.-M. Wang, W. Wang, A.-L. Hu, and S. Shen, "Statistical cross-language Web content quality assessment," *Knowledge-Based Systems,* vol. 35, pp. 312-319, 2012.

[62] K. N. Qureshi and A. H. Abdullah, "A survey on intelligent transportation systems," *Middle-East Journal of Scientific Research,* vol. 15, pp. 629-642, 2013.

[63] K. N. Qureshi and A. H. Abdullah, "Adaptation of Wireless Sensor Network in Industries and Their Architecture, Standards and Applications," *World Applied Sciences Journal,* vol. 30, pp. 1218-1223, 2014.

[64] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, "Security Issues and Attacks in Wireless Sensor Network," *World Applied Sciences Journal,* vol. 30, pp. 1224-1227, 2014.