Measuring the Effectiveness of Phishing Detection Tool: Comparative Study on Pattern Matching and User Rating Technique

Sharifah Roziah Mohd Kassim*, Md Sahrom Abu, Amirah Mohd Omar
MyCERT, Cybersecurity Malaysia, 43300 Seri Kembangan, Selangor D.E, Malaysia.

* Corresponding author. Tel.: 603-8992 6888; email: roziah@cybersecurity.my
Manuscript submitted January 21, 2019; accepted March 12, 2019.
doi: 10.17706/jcp.14.4.302-310

Abstract: Phishing incidents continues to increase each year and becoming a global threat despite of having phishing detection tools in place. Successful phishing attacks are causing huge loss of money to Internet users and financial Institutions globally and several anti-phishing tools had been proposed to mitigate against phishing. A popular phishing detection tool currently used is the user rating technique, in which users will submit suspicious phishing URLs to a Phishing Blacklist Database, that for verification if it is phishing site. However, it is unclear to the effectiveness of this mechanism in detecting a suspicious site as a phishing website and in mitigating phishing attacks. The shortcomings and setbacks to this approach, in some aspects, needs to be improved and for this purpose, this paper proposes a new phishing detection tool which uses pattern matching technique in detecting a suspicious site as a phishing website. Our findings from this paper will be looked in terms of the speed of detection, false alarm, accuracy and interdependability in comparison to the current phishing detection tool.

Key words: Anti-phishing, phishing, pattern matching, user rating

1. Introduction

The use of the internet has grown in our daily lives; many services are now available online. This new business market offers many opportunities for service provider, online entrepreneurs including financial institution. This is a great facility and is useful especially for those that are too busy with work and could not leave their desk to even pay the bills. They will use these online services everywhere. However, it is also an advantage for the criminals and without realising, various web pages with malicious intends like phishing and online scam emerged at the same time.

A phishing attack is a criminal activity which mimics a certain legitimate web page using a fake web page to lure end-users to visit the fake website and stealing their personal information such as username, passwords and the credit cards credentials. This is supported by Anti Phishing Working Group (APWG) that phishing is a criminal mechanism employing in both social engineering and technical subterfuge to steal customer's information and financial credentials. Phishing email is a category of spam, an unsolicited email message, sent to multiples users to lure them to provide their online identities for impersonation [1]. Phishing attacks involve three major phases: The first is potential victims receiving a phish; the second is the victim taking the suggested action in the message, usually to go to a fake Web site but can also include installing malware or replying with sensitive information; and the third is the criminal monetizing stolen information [2].

Phishing attacks normally happen at online banking or while doing online shopping. According to the Anti-Phishing Working Group (APWG) report and based on Fig. 1, payment gateway and financial institution are the largest attack by an attacker which is 42% and 15% respectively [3].

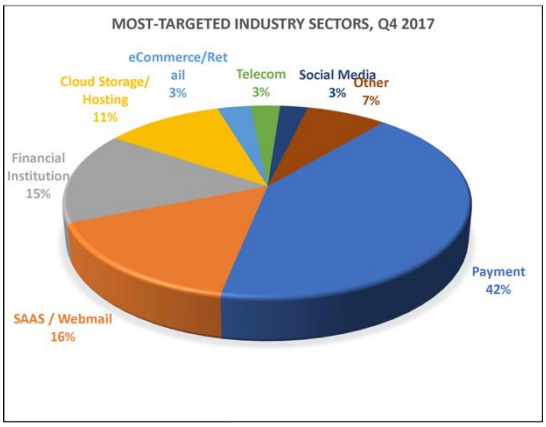

Fig. 1. Percentage of industry that being attack.

Criminals often use email as a tool to conduct phishing attacks by sending spam emails or masquerading as a legitimate bank to attack the victims. The email's content will trap users into a fake website to disclose personal information[4]. From report APWG, there were at least 180757 unique phishing attacks worldwide seen in quarter four of 2017 [3]. Phishing has become a major criminal activity involving money and personal data.

Although user awareness remain the strongest and at the same time, the weakest link to phishing countermeasures, [5] a lot of methods have been proposed and developed to protect against phishing attacks such as stopped communicating with customers via email. Other than that, an anti-phishing tool had been programmed by developer as a method to detect phishing from user's browser such as SpoofGuard, Netscape, Netcraf, and Ebay. Unfortunately, these approaches are susceptible to attacks launched from compromised legitimate website [6].

Statistics by Malaysia Computer Emergency Response Team (MyCERT) as shows in Fig. 2, recorded phishing attacks by years.

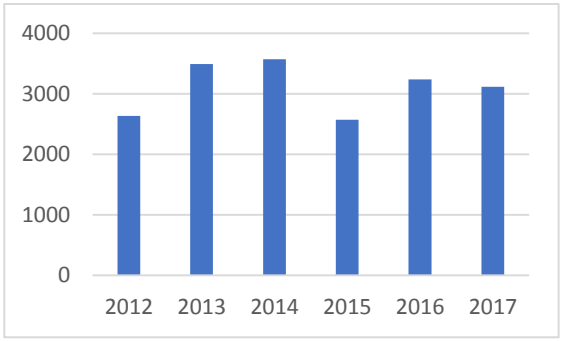

Fig. 2. Statistics on phishing incidents in Malaysia.

According to Bank Negara Malaysia (BNM), there was a case whereby the bank loses 0.00002 % from any bank transaction in year 2008 caused by phishing. In the first six months of 2009, there was 1191 fraud case involving RM 1 million transferred through online banking. Phishing has caused lots of economic losses. In Malaysia, phishing is still categorized as major threat online banking with a total of 94 percent of the complaints received. Based on these statistics, users in Malaysia should be more aware about phishing attacks and double up the effort to protect themselves from being victimised by this cybercrime. In order to

prevent Malaysian user's being attacked by phisher, Cybersecurity Malaysia had developed Don't Phish Me, an anti-phishing tool for Malaysians online banking users. Section 2 of this paper will look into the objectives of why the research is conducted, followed by Section 3 which highlights on some of the previous works that had been done by Researchers on this area. Sections 4 and 5 describes in details of the two techniques discussed and made comparisons in this paper, which are the user rating and pattern matching techniques. Section 6 looks into the results and findings after implementing the proposed technique which is the pattern matching technique in a few aspects such as in terms of speed and accuracy of detection. The final section of this paper, Section 7 will conclude this paper based on results and findings.

2. Objectives

This research paper is conducted with the objectives as mentioned below:

1. Highlight shortcomings of current phishing detection mechanisms.

2. To propose a more effective phishing detection solution that improves the current phishing detection mechanism.

3. To safeguard the public and Financial Institutions phishing attacks that causes huge money loss to affected parties.

3. Related Work

Phishing attacks are still prevalent no matter in Malaysia or abroad. Phishing attacks have increased and becoming sophisticated based on statistics by MyCERT. There are quite a number of phishing solutions have been developed to tackle the problem. A method used by one of the anti-phishing solutions is to initially identify the phishing target to determine whether the suspicious webpage is a phishing page.

Table 1 summarized the related works in detecting phishing sites that being used.

Table 1. Related Works on Phishing Technique

Techniques	Strength	Weakness
TF-IDF (term frequency / inverse document frequency) information retrieval algorithm.	95% correctly define as phishing website	Does not work well with East Asian language
Exploit Hypertext Mark-up Language Document Object Model, Search Engines, a machine learning algorithm and PhishTank	92% correctly define as phishing website	High false positive outputs
Automated Individual White-List (AIWL)	Warning user probably under phishing attack if the ID is not in white list	List is being controlled
Sends a large number of bogus credentials	Hiding real credential	Too many credentials needed
Fuzzy algorithm data – mining with 27 features and six criteria.	83.7% accuracy	Neil
Neural Networks	Neil	Not enough time to produce result
Adaptive Neuro-Fuzzy Inference System	First study to demonstrate the effectiveness of phishing e-web-form features 98.4% correctly define as phishing website	Manual selection for phishing characteristics identification

P. Prakash *et al* [7], designed a system named PhishNet, which has two components. In the first component, five heuristics were suggested to enumerate simple combinations of existing phishing URLs in order to uncover new phishing URLs. The other component consists of an approximate matching algorithm that dissects a URL into multiple components which are than matched individually against the URL entries in the blacklist.

CANTINA [8] had proposed to detect phishing web page based on the TF-IDF (term frequency / inverse document frequency) information retrieval algorithm. They also used heuristics to reduce false positive. They were finding a good result approximately 95% correctly of phishing sites. However, there is limitation on this approached since TF-IDF does not work well with the East Asian language. Xiang et al has proposed [9] a new method enhance from CANTINA that includes 8 novel features which exploit the HTML Document Object Model (DOM), search engines and machine learning hence the birth of CANTINA+. Among the 15 features they have used are Hypertext Mark-up Language Document Object Model, Search Engines, a machine learning algorithm and PhishTank. The results are 92 % accurate but the approach suffers high false positive outputs.

CAO using a novel anti-phishing approach named Automated Individual White-List (AIWL) [10]. AIWL trying to maintain a normal user whitelist check into a certain website. When users sign in to LUI (Login user interface), if the ID is not in the white list, AIWL will give a warning to users are probably under phishing attack. The white list however is being controlled and the entire application will lose its effectiveness. The weakness of this approach is, it will be a problem with the PC security tools in it.

In their study, Yue and Wang [4] designed a BogusBiter which is a client-side tool, which sends a large number of bogus credentials to suspected phishing sites, hiding the real credential among the bogus ones. Another, smart phishing detection has been developed by Aburrous *et al* [6]. Their approach is based on fuzzy algorithm data – mining with 27 features and six criteria. The approach achieved 83.7% accuracy. However, this approach has features that are not sufficient. A similar framework for predicting phishing web was proposed by Martin *et al* [11]. In their approach, Neural Networks have been used for training and testing in order to predict the performance of their systems. They found that phishing site stay only for a 2 and half day before being taken down. Unfortunately, the official results are not presented, making it difficult to review their performance.

Moreover, Barraclough *et al* [12] used Adaptive Neuro-Fuzzy Inference System to analyses and combines phishing emails and phishing web-forms in a single framework, which allows feature extraction and feature model construction. The outcome should classify between phishing, suspicious, legitimate and detect emerging phishing attacks accurately. In this study, 2-fold cross-validation is used randomly by splitting the features into two parts, training set and testing set. The limitation in this study is it require manual selection for phishing characteristics identification due to phishing strategy that evolves regularly.

4. User Rating Technique

Some anti-phishing provides users rating as method or mechanism to detect phishing site. The current methodology of anti-phishing used is displaying a risk rating between one to ten as well the web hosting location site. The risk rating evaluates site's characteristics by comparing against described fraud sites and grade it using rating ranging from "0 to 10" where zero (0) indicates secured site and ten (10) indicates it's a phishing site. This mechanism work is based on URLs reported by user. The URLs are then stored in a database and when the site gets higher submissions through the tool, the site is automatically suspected as a phishing website and blocked users from browsing those pages. Limitation of this mechanism is the user may ignore the warning and continue to browse the website since the indicator does not automatically block the phishing website because it will only produce the ratings. This is data flow how the mechanism works.

5. Pattern Matching Technique

In this research, we are proposing an anti-phishing tool which utilizes the pattern matching technique to detect phishing websites on a real time basis and prevent end users from releasing their credentials to the phishing website.

DontPhishMe is an initiative of MyCERT, CyberSecurity Malaysia, to provide a security mechanism in preventing online banking phishing threat specifically for local Malaysian banks. DontPhishMe is an addon to Firefox that alerts you if an online banking web page that you visit appears to be asking for your personal or financial information under false pretenses. This type of attack, known as phishing or spoofing, is becoming more sophisticated, widespread and dangerous hence the importance to browse safely with DontPhishMe. DontPhishMe will automatically warn you when you encounter a page that is trying to trick you into disclosing personal information.

DontPhishMe is a name of the anti-phishing tool. DontPhishMe will automatically warn user when they encounter a phishing site. This anti-phishing tool provides security mechanism to protect online banking phishing site specifically for local Malaysian banks. Fig. 6 explains the works of DontpPhishMe. If the user encounters a possible phishing site, DontPhishMe will automatically checks the URL with selected whitelist. If the URL is found listed, it will redirect the page as normal. If not, DontPhishMe will continue to execute the pattern matching technique to further analyze the website. The algorithm will compare certain attributes selected between the phishing site and the authentic site. Once the threshold hits more than 80% dissimilarity, it will automatically block the page requesting to leave the phishing website. Once the user decides to leave the phishing website, DontPhishMe will disable all inputs and redirect to the safe page of APWG. If less than 80% dissimilarity, the page will resume as normal.

Fig. 3, Fig. 4, Fig. 5 and Fig. 6 demonstrated how the Alert Message triggered by DontPhishMe when users unknowingly visit a phishing website.

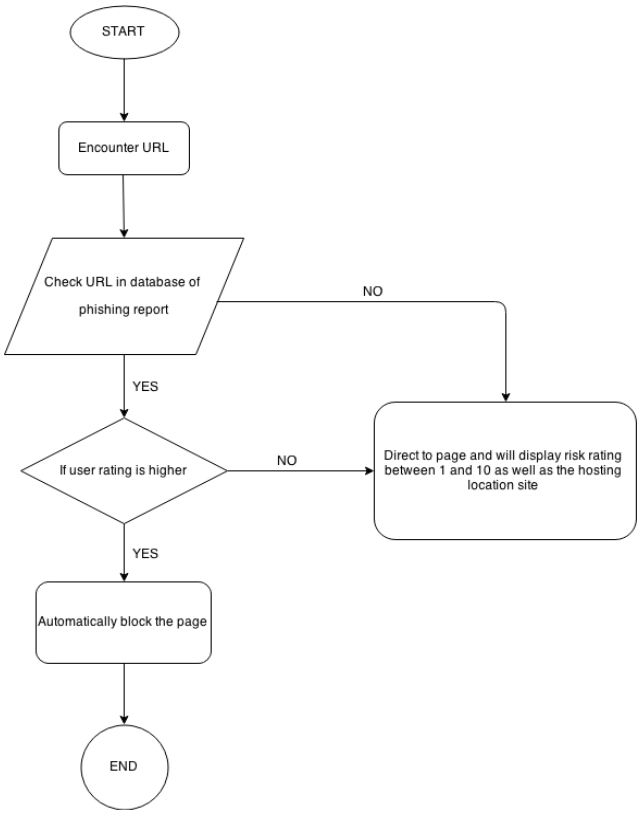

Fig. 3. Data flow user rating technique.

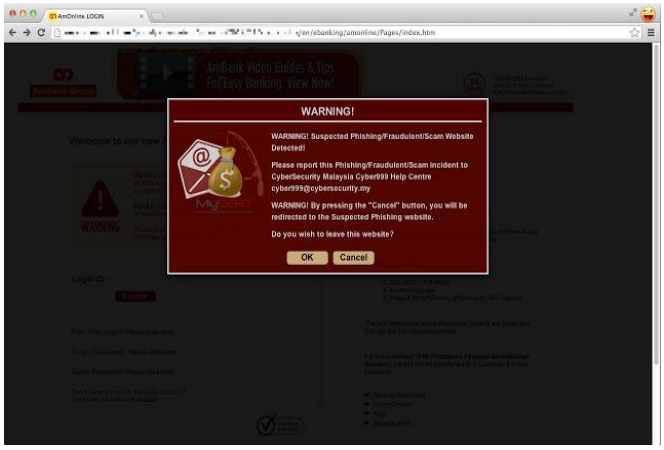

Fig. 4. First warning received.

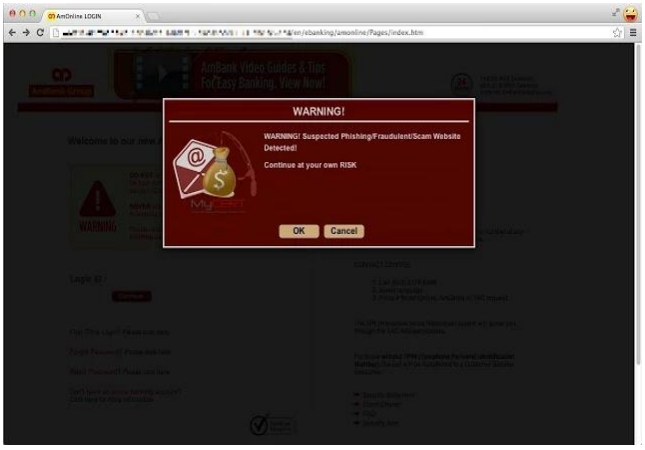

Fig. 5. Second warning received.

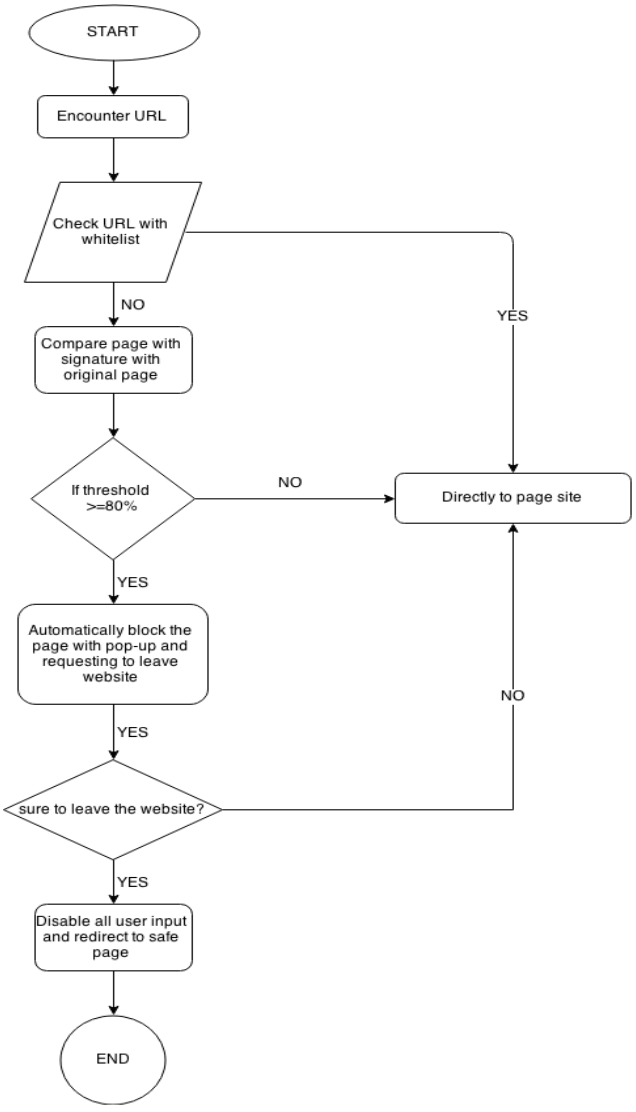

Fig. 6. Data flow pattern matching.

Fig 7 shows the statistics for phishing URL that has been detected by DontPhishMe started from 2012. The graph shows that DontPhishMe implementation has helped to reduce the number of phishing URL or phishing site in Malaysia.

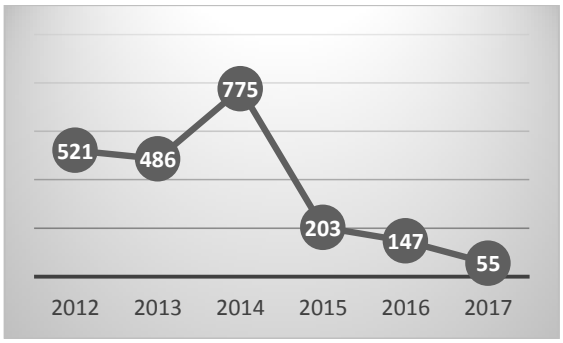

Fig. 7. Statistics on phishing URLs detected by DontPhishMe.

6. Results and Findings

After the implementation of using the proposed phishing detection mechanism in comparing with the current detection mechanism, we found an increase in rate of proficiency in detecting phishing sites in a fast and accurate manner. The current mechanism failed to detect a phishing website but DontPhishMe successfully detected the phishing website. Fig. 8 and 9 illustrates the failed and successful detection.

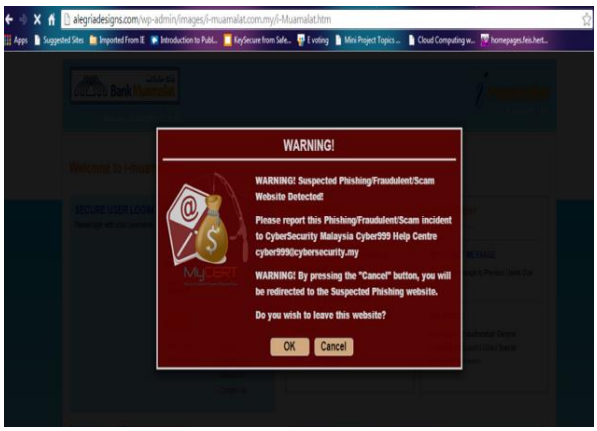

Fig. 8. Successful detection of phishing website by DontPhishMe.

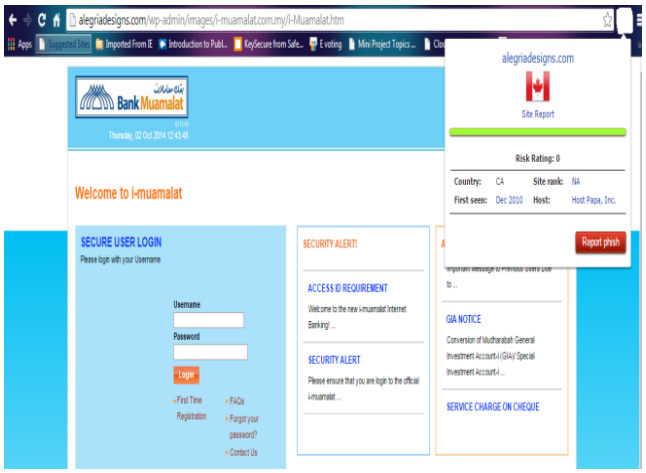

Fig. 9. User rating mechanism failed to detect phishing website.

In this research we had tested several accessible phishing websites that are still alive, using both mechanisms to measure the effectiveness of successful detection. The test result is presented in Table 2 below:

Table 2. List of Phishing URL Detection Results

URL	Detection on phishing site	
	Pattern Matching mechanism	User rating mechanism
http://alegriadesigns.com/wp-admin/images/i-muamalat.com.my/i-Muamalat.htm	yes	no
http://sellmyskills.com.au/gallery_uploads/M2u/M2ULogin.doaction=Login.html	yes	yes
http://beckydimattia.com/photoblog/wp-admin/network /m2uSession/m2uSession/m2uSession/Welcome.html	yes	yes
http://ultrastream.my/wp-includes/images/smilies/ m2uSession/m2uSession/m2uSession/Welcome.html	yes	yes
http://s84.n44.n171.n68.static.myhostcenter.com/ wp-content/plugins/10421312312/index.html	yes	no
http://203.106.226.91/Login/lgn_new.aspx	No	no
http://alegriadesigns.com/wp-admin/images/ i-muamalat.com.my/i-Muamalat.htm	yes	no

The results and findings are captured as in the below Table 3.

Table 3. Findings and Result from Using Both Mechanisms

	Current Mechanism	Dontphishme
Accuracy	Low	High
Speed	Low	High
Probability of Becoming Victim	Average	Very High
Detection Capability	Low	Very High
Probability of False Alarm	High	1.98%
Interdependency	High	Low

Based on the results and findings, we found by proposing the new mechanism, yields the below overall advantages for more effective detection of phishing websites and reduce the probability of end users becoming victims:

a) Accuracy in detecting the phishing website. We found the new mechanism has high accuracy of detecting a phishing website compared to the current mechanism. This is because DontPhishMe detects based on real time pattern matching and is not dependent on third party verification. This helps end users to identify a phishing website immediately and prevent them from login into a phishing website.

b) DontPhishMe immediately detects a phishing website on real time basis as it does not require third party verification.

c) Preventing User to Login to a Phishing Website. Apart from detecting a phishing website, the proposed tool also prevents user to key in their credentials in the login page after the third phishing website alert message by the tool. The existing mechanism lacks this ability.

d) Detection engine. The proposed tool uses pattern matching technique to detect a phishing website in a real time basis which is much more effective compared to the current mechanism which is based on pre-defined whitelisting/blacklisting of phishing websites.

e) Dependency. The proposed tool is not dependent on a third-party verification of phishing website where else the current mechanism is dependent on a third-party verification which actually affects the quick identification of phishing websites.

7. Conclusion

Based on the results and findings of this research paper, the proposed phishing detection mechanism is found to be an effective alternative for detecting phishing sites more efficiently with increased accuracy, less false detections and fast compared to the existing mechanism. The proposed mechanism is also predicted to reduce incidents of Internet users becoming victims of phishing. In addition, the proposed mechanism also prevents end users from becoming a victim by disabling typing functionality on the phishing website.

Our future plan on this research is to study on the possibility to reduce the occurrence of false alarm during detection. Our proposed study is to by increasing the algorithm of the current pattern matching technique to reduce the occurrence of false alarm. Some initial studies will be conducted on this research together with tests and experiments.

References

[1] Nagunwa, T. (2014). Behind identity theft and fraud in cyberspace: The current landscape of phishing vectors. *International Journal of Cyber-Security and Digital Forensics*.

[2] Hong, J. (2012). The state of phishing attacks. *Commun. ACM*, *55(1),* 74.

[3] APWG. (2017). *Phishing Activity Trends Report Q4 2017*.

[4] Yue, C., & Wang, H. (2010). BogusBiter: A transparent protection against phishing attacks. *ACM Trans. Internet Technol.*, *10(2),* 1-31.

[5] Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. *Int. J. Secur. its Appl.*

[6] Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Experimental case studies for investigating e-banking phishing techniques and attack strategies. *Cognit. Comput.*, *2(3),* 242-253.

[7] Prakash, P., Kumar, M., Rao Kompella, R., & Gupta, M. (2010). PhishNet: Predictive blacklisting to detect phishing attacks. *Proceedings of IEEE INFOCOM*.

[8] Zhang, Y., Hong, J., & Cranor, L. (2007). Cantina: A content-based approach to detecting phishing web sites. *Proceedings of Conf. World Wide Web* (pp. 639-648).

[9] Xiang, G., Hong, J., Rose, C. P., & Cranor, L. (2011). CANTINA +: A feature-rich machine learning framework for detecting phishing web sites. *ACM Trans. Inf. Syst. Secur.*, *14(2)*, 21.

[10] Cao, Y., Han, W., & Le, Y. (2008). Anti-phishing based on automated individual white-list. *Proceedings of the 4th ACM Workshop on Digital Identity Management - DIM '08* (p. 51).

[11] Martin, A., Anutthamaa, N. B., Sathyavathy, M., Saint Francois, M. M., & Venkatesan, P. (2011). A framework for predicting phishing websites using neural networks. *Int. J. Comput. Sci. Issues*, *8(2),* 330-336.

[12] Fehringer, G., & Barraclough, P. A. (2017). Intelligent Security for Phishing Online using Adaptive Neuro Fuzzy Systems. *Int. J. Adv. Comput. Sci. Appl.*, *8(6),* 1-10.

Sharifah Roziah is a specialist for Malaysia Computer Emergency and Response Team (MyCERT) under the umbrella of CyberSecurity Malaysia where she is also tasked as a manager of the Security Operation Centre to ensure computer security incidents are responded to in a timely and efficient manner.

Md Sahrom Abu is a senior analyst at MyCERT, Cybersecurity Malaysia. His main task is focusing on cyber threats and research. He graduated from University of Teknologi, Malaysia for his bachelor degree. Currently, he is pursuing a postgraduate degree.