Enrich Awareness of Users to Detect Phishing Websites

Muhammad Dawood, Othman Bin Ibrahim, Waheeb Abdel Rahman Ali Abu-Ulbeh

Abstract: ***Phishing attack is used for identity theft with the help of social engineering and some sophisticated attacks. To attract the user by clicking a URL and is trapped to a phishing Web page. Security for user's credentials is one of most important factor for organizations nowadays. It can be achieved through several ways like education and training. Through training and education the level of awareness will be increased also it helps to mitigate phishing. Approach with several steps is introduced in this paper, where a user must take a look or take these precautionary measures if the user is browsing any Web browser. We found it possible to detect Phishing Web pages without anti Phishing solutions. This approach contains several steps to examine whether the Web page is a real Web page or a fake Webpage. All these steps will check the phishing features exist in that Web page or not. For evaluation of our approach we analyzed the data set of Phish Tank, this data set is full of Phishing Web Pages. The purpose of evaluation is to check the features discussed in our approach to aware the user. From the following result it is resulted that the user can detect without using any Anti Phishing solution just by taking some steps to check the Web page for certain features.***

Index Terms**:** ***Keywords: URL, Phishing, Phish Tank, CA (Certificate Authority), Webpage.***

I. INTRODUCTION

Internet is one of the important ways to communication among the people. A lot of people are using the internet to manage their online business or use it as a complementary support to their offline business. People can use the internet for various purposes such as sending emails, e-banking activities, selling or buying products weather it is a digital or concrete products. In addition, people can use the internet to engage in political issues or social activities. In spite of all of these advantages of the internet, however there are some disadvantages which can be negative to people. When the people connect to the internet, they will be under threat because of different online frauds. Internet fraud is a kind of crime which is conducted online. Internet fraud has many ways in order to deceive the users who involved in online activities. That's why internet is a very good way to trick the users who use it to Purchase products or services [9].

Currently, online business is a part of internet and without security it will be difficult to run online businesses and that's why security solutions have been established. Always there is a way to violate the security solutions and it would result in unpredictable consequences. The results can affect users, companies and even organizations. It was revealed that $3.4 Billion Online Revenue Loss Due to fraud in 2011 [10].

Internet fraud has been changed or improved by attackers. Nowadays it has different types and tools to perform. And it became more complicated which is not easy to terminate. Recently, attackers found a lot of obstacles regarding to the security solutions so they cannot conduct Internet fraud simply. And most of them they want illegal profits form easy way. That's why they have been involved in phishing emails and websites to trick the users and make illegal profits.

As it is mentioned above that internet fraud has many ways in order to trick the user, Phishing attacks are developed in many ways. Phishing is a kind of attack that belongs to social engineering and this attack seeks to trick people in order to let them reveal their sensitive information. Sensitive information might be about themselves or their accounts such as credit cards, login information of a particular system or banking accounts. Phishing can trick the people by taking advantage of how the people interact with computers rather than exploiting system vulnerabilities [6].

Distinguish between phishing and legitimate website can be done by investigating several characteristics. 27 website features are pointed out which can be investigated to detect phishing websites [1]. These features are categorized into six categories and each category includes several components needs to be checked. But in this paper we will only emphasize on features where user can detect them easily.

II. BACKGROUND AND PREVIOUS WORK

In this section we will explain some of the techniques for detecting phishing attacks previously. Add-in tool bars for the browser is one of the most popular methods of detection. Spoof Guard tool is also one of the tools for detection [3]. This determines the legitimacy of URL and Domains. Another tool presented, for protecting identity and password information [7]. Defining the personal information of client in terms of password, username and email address then introducing a function which provides a client with different personal information for different servers by its visiting. A tool Pwd Hash is a similar concept introduced later.

There are some other tools which include Google safe browsing, Net Craft tool bar, Spoof Stick, and Site Advisor. Most of them are tool bars and they rely on the information black listed and may be correctly are not able to identify new Phishing attacks. In comparison of our approach it enhances the awareness of every user who browses the browser.

Revised Manuscript Received on September 22, 2019.

Muhammad Dawood, PhD student in faculty of computing at UTM,Malaysia, mastangalbaloshi@gmail.com

Othman Bin Ibrahim, Associate Professor in faculty of Computing at UTM, Malaysia

Waheeb Abdel Rahman Ali Abu-Ulbeh, PhD from UTM, Malaysia

A thorough analysis was performed on anti-phishing tool bars to find out their effectiveness [11]. Suggestion was after finding that Spoof Guard was much effective for phishing site detection, though it was having a high false positive rate. It does not rely of white and black list information. But its result showed that phishing URL freshness affected the performances many phishing tools that rely on black list information.

Another approach is visual appearances of Web page, by introducing a dynamic security skin technique [5]. Human Interactive Proofs it was an extended implementation. In this technique a shared secret image that proves its identity to a user by allowing a remote server.

Trust Bar was proposed which is a third party certification solution to mitigate phishing [8]. From Anti-phishing work group database 200 phishing attacks were analyzed and different reasons were identified, which showed that lack of computer system knowledge, opponents using visual deception tricks make users fall in to phishing attacks [4].

None of the previous work has emphasized the awareness especially for the user who is browsing internet publically. Mostly their solution were remote based database to detect phishing Web pages if there is any new type of phishing attack cannot be detected. But in our work we emphasized on the public user who can be anyone, he by just looking on the Web pages and following several steps can judge phishing Web pages.

III. PHISHING WEBSITES CHARACTERISTICS

There are various characteristics to detect phishing websites. First part of these characteristics concerning to the URL of the website and other part is associated to the HTML source code. Below we discussed in detail only the characteristics that the user can detect them by only looking at it.

A. Using the IP Address

Normal case is to see a domain name which can be presented by characters or numbers but it should start with www and end with one or two dots. From domain name the user can confirm his destination for surfing. The main function of domain name is connecting to the server IP so the user does not need to know the IP. For instance, www.paypal.com it is a domain name and it shows the destination to the user clearly. In order to confuse the user where he is, hackers hide the destination Website by replacing the domain name with IP address. For instance, http://198.164.11.30/en/ this IP address can present a website instead of domain name.

B. Using SSL Certificate

Usually, most of phishing websites try to impersonate important website such as e-banking, so these legitimate websites must have SSL certificate and it is included in the URL for example https://www.paypal.com. As a result some phishing websites do not have “s” letter after http to tell us this communication is secure.

C. Certificate Authority

SSL certification contains the identity and any relevant information presents the owner. In surfing case, the browser will ask the server to present the certification. Legitimate website will send back to browsers a certificate which contains the identity and relevant information. But in phishing website case, the certificate which will be sent back to browser will contains wrong data such as the URL, because in this case the phishing website will send a copy of certification of the legitimate website [5] .

D. Spelling Errors

Spelling Errors often use by phishing email in order to escape from spam and phishing filter. Spelling errors can be as mistakes in spelling, grammar, and logic gaps. Surly, Legitimate website will not have these kind of errors and they will use professional language to communicate with their customers. In general, these types of intentionally mistakes are difficult to detect because it might be in different way so these mistakes supposed to be detected by human or in another word by customers themselves [2].

E. Using Forms With “SUBMIT” Button

Usually, most of legitimate websites use the forms only for login process or any registration or subscription process. But phishing websites used to include a number of forms with a submit button which might have hidden variables to send it to the destination file or to redirect the user to a different page. And they used to do it because it is the easiest way to send hidden information. Obviously the user cannot know the destination of his credential information unless he checked the source code of the webpage.

IV. APPROACH

In our approach we are giving awareness to the user when he will open the Web browser which can be of any kind like Firefox, Internet Explorer or Google Chrome. So if the user types or searches any of the Web page the browser will open the said Web page, when the Web page is opened by the browser now this is the time that user has to give attention on this suggested approach. This approach contains several steps to examine whether the Web page is a real Web page or a fake Webpage (for Phishing).

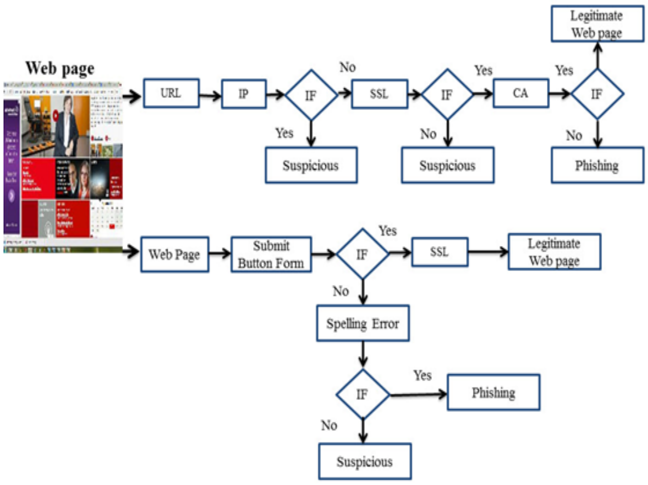

Fig.1. Approach for Detecting Phishing by Users

This approach is opted without using any Anti Phishing solution tool to be brought in. so when these steps are taken by the user for sure he will be safe at least not being victimized by the phishing Web pages, mostly people get trapped by just clicking. By taking these following steps the user can secure him from being a phish.

The first step that the user should take after the Web page has been brought by the browser is to have a look at the URL as shown in Fig.1. If the URL is written as it is like the domain name he desired then he can proceed, if he sees an IP address then he must suspect that why this site showed like as an IP address. Now, he should check the SSL (secure socket layer) connection, if the SSL connection is missing or not provided then it will also be taken as suspicious Web page. If the connection is provided then he must check the next step which is CA (certificate authority) if the CA is verified like from VeriSign then it means it is verified and not a phishing Web page. Otherwise, it is a Phishing Web page.

In this approach the next step for the user to check the content of the Web page browsed by the browser. To see whether is there any submit button if there is a button to submit a form or something like that then the user should take these precautionary measures to see by himself that whether it is a phishing Web page or the real Web page. Now if there is a button for submission he must check the SSL if there is SSL provided then it is a legitimate or real Web page. If there is no button for submission then check whether there is any spelling error if yes then it is for sure a phishing Web page, if no then the user must suspect that this page is a suspicious page.

V. RESULTS AND DISCUSSION

For evaluation of our approach we analyzed the data set of Phish Tank, this data set contains number of Phishing Web Pages. The purpose of evaluation is to check the features discussed in our approach to aware the user. And the most features selected in this evaluation process which are easily checked by the user and are mostly involved in Phishing activities. This data set has shown some results which are shown in Fig. 2.

The data set from Phish Tank showed the following result which approves our approach. The result showed that mostly Phishing Web pages have Submit button or forms. So user can easily recognize this feature. And after that the feature easily detected by the user is SSL, if it's not provided by the Web pages which mean these Web pages are Phishing Web pages. IP address is not so important because Phishing Web pages like shown in the result just some use IP address as Phishing purpose not all. That is the main reason in our approach we paid less attention to the IP address.

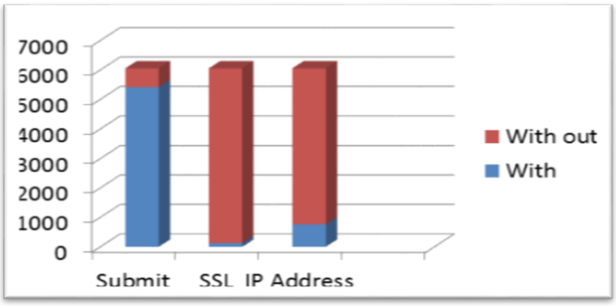

Fig.2. Analysis of Phish Tank Data Set.

VI. CONCLUSION

This suggested approach is targeting mainly the normal user not user for a specific organization to train them. This paper will increase the awareness of normal users who browse internet publically. From the Phish Tank data set result it is resulted that the user can detect without using any Anti Phishing solution just by taking some precautionary steps to check the Web page for certain features. These steps are just by looking without any tools to execute. And can save him from being Phishing victim. In future our plan is to consider some more features as the world of internet is growing rapidly, and also we will consider not only the normal user but also the users from specific organizations or technical users too.

ACKNOWLEDGEMENT

I would like to thank Associate Professor .Dr.Othman Bin Ibrahim for his guidance and support. The knowledge I have acquired is invaluable and the challenges that we have faced proved to be a very enriching experience to my career.

REFERENCES

[1] Aburrous, M., Hossain, M., Dahal, K. and Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. Expert systems with applications, 37(12), 7913-7921.
[2] Blythe, M., Petrie, H. and Clark, J. A. (2011). F for fake: Four studies on how we fall for phish. Paper presented at the PART 5--------Proceedings of the 2011 annual conference on Human factors in computing systems.
[3] Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D. and Mitchell, J. C. (2004). Client-side defense against web-based identity theft. Paper presented at the 11th Annual Network and Distributed System Security Symposium (NDSS'04).
[4] Dhamija, R. and Tygar, J. D. (2005). The battle against phishing: Dynamic security skins. Paper presented at the ACM International Conference Proceeding Series.
[5] Dhamija, R., Tygar, J. D. and Hearst, M. (2006). Why phishing works. Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.
[6] Downs, J. S., Holbrook, M. B. and Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. Paper presented at the Proceedings of the second symposium on Usable privacy and security.
[7] Gabber, E., Gibbons, P. B., Kristol, D. M., Matias, Y. and Mayer, A. (1999). Consistent, yet anonymous, Web access with LPWA. Communications of the ACM, 42(2), 42-47.
[8] Herzberg, A. and Gbara, A. (2004). Trust bar: Protecting (even naive) web users from spoofing and phishing attacks. Computer Science Department Bar Ilan University, 6.
[9] Philippsohn, S. (2001). The dangers of new technology—laundering on the internet. Journal of Money Laundering Control, 5(1), 87-95.
[10] Wen, L. (2012). Linkage of Cyber Source to Promote Entrepreneurship and Employment of College Students Baoding City College Students" Internet Survival" Status Investigation. Journal of Baoding University, 1, 014.
[11] Zhang, Y., Egelman, S., Cranor, L. and Hong, J. (2006). Phinding phish: Evaluating anti-phishing tools.

AUTHORS PROFILE

My name is Muhammad Dawood, and I am PhD student in faculty of computing at UTM,Malaysia, for more details contact me mastangalbaloshi@gmail.com

I am Othman Bin Ibrahim, working with Associate Professor in faculty of Computing at UTM, Malaysia

My name is Waheeb Abdel Rahman Ali Abu-Ulbeh, and doing PhD from UTM, Malaysia.