Australian Academy of Business and Economics Review
Volume 2 ● Issue 1 ● January 2016

www.aaber.com.au

Phishing Attack Detection Using Taxonomy Model

Chowdhury Sajadul Islam
Uttara University, Bangladesh

Abstract

The objective of this paper is to detect phishing threats by using our proposed threat taxonomy model. To propose this threat taxonomy model, we have derived four different equations to calculate the predicted rate of phishing threat parameters that are used for phishing attacks. We have collected the information on phishing attacks by applying various methodologies, building an intellectual data set and experimenting on these data sets. We have done the experiment on the basis of our collected data sets and putting the values in four different equations which gave us the predicted rates of a phishing threat parameter such as; method, origin, component and target in respect of predicted number of threats. Experimenting on the intellectual data set, we got numerical results which are represented graphically. Finally, we got a phishing threat taxonomy model which demonstrates in a tabular form. The results show that even if some of the phishing threats' methods, components and origins are different, the website can still be phished and forged, and users should be aware while dealing with it. Our proposed model showed a high heuristic accuracy for detecting the rate (%) of phishing attack when we applied our phishing detector software.

Keywords: Phishing Attack; Phishing Origin; Malware Attack; Phishing Target; Taxonomy Model; Phishing Attack Detection

1. Introduction

Phishing is nothing but fooling people by snatching user credentials in an illegal way. The impact of phishing attacks is deadly on the financial sector. There are lots of phishing threats available in the phishing world which are *fake websites*, *link manipulation*, *pharming*, *in session phishing*, *spear phishing* etc. The first four attacks are mainly web based [1-2]. In *fake website* attacks, [3-4], a domain name is purchased that is very much similar to a legitimate site.

When the victim visits those fake sites, he/she loses his or her credentials. In *Link manipulation* attacks, [5, 3] some common tricks like misspelled *url*, link anchoring etc. are used to mislead the users to fake sites. In *fake popup* attacks, real website loads, a *pop up* coming from the sites asks the user to give his/her credentials. In *fake websites with validation* attack, the victim enters user credentials to the fake site and sends the credentials to the real site and it automatically validates whether the user name and password provided is correct or not [3]. A *Pharming* attack [3-4], redirects the victim to the fake site even though the victim enters the correct address for the legitimate website. *In-session phishing*, [3-5], the phishers inject malicious *Java Script* with legitimate websites so that when customers visit one of those sites during online banking, he gets targeted. *Spear phishing* attacks are usually carried out via a targeted *email*, sent with either a malicious attachment or with a link to a malicious website. There are more phishing attacks which are *phone calls*, *Evil twins*, *Malware-Based Phishing*, *Search Engine Phishing* and *Internationalized Domain Names* (*IDN*) attacks which also have negative purposes. We have done our experiments on most of the attacks to build the rate of phishing threat parameters that finally helped us to propose the threat taxonomy model [6].

2. Background

Over the years, a lot of experiments, studies, researches have been conducted and tools have been developed to combat the phishing threats, yet the rate of phishing attacks are consistently increasing [1,14]. During FIFA world cup 2014, [1] phishers had sent personalized e-mails, link, messages to victims saying that they had won a World Cup game ticket. After[7] conducting a comparative experiment on phishing and non-phishing URLs, using parameters like IP addresses, URLs (length, character distribution, and presence of predefined brand names) it was found that phishing and non-phishing URLs are different in length and misuse of free hosting services by phishers. Phishing URLs were classified using CANTINA, a tool used for analysing the following content of the webpage [8] such as assigned a weighted sum of 8 features (4 content-related, 3 lexical, and 1 WHOIS-related) to build the classifier. Further, they developed 8 discriminatory features and proposed CANTINA+ [8-9].

3. Experimental Setup of Phishing Taxonomy Model

The main theme of the threat taxonomy model of phishing attack is taken form Biology. In this paper, we have proposed the threat taxonomy model of phishing attacks in table V, which can effectively detect the different categories of phishing attacks. The functional descriptions of the threat taxonomy model's parameters are given below:

Method- refers to how the attack happens and also determines the weakness in the environment that may have allowed the attack to take place

Origin- works as an identifier in the phishing attack taxonomy model which is able to detect the origin of all available phishing attacks. The origin of most of the categories of phishing attacks are respectively software, human and physical.

Threat Component-can be tools, applications, languages, APIs, software and people.

Target-suggests to experiment the past threat behaviour, specifically its effect and then finds out the target of the attacks. For example, target of the phishing attack is to make financial gain, and fooling the user.

In this paper, we have conducted the experiments on various data sets including both phishing and legitimate sites [6, 10] retrieved from various databases such as ACM Digital Library [9, 11], Springer Link [7], IEEE Xplore [12], Science Direct [13], Google, Google Scholar, and Yahoo. We have also holistically examined phishing attacks in various stakeholders and their counter measures, and by surveying experts' [15] opinions about the current and future threats, [1, 14] to propose this model. By using our equations (1-4), we get the rate of phishing attack which consists of four parameters such as origin, method, threat component and target. We have individually examined each parameter of phishing attacks, the results of which are presented in table V. Basically, the more effective a heuristic, the higher the percentage of phishing threat occurs from miss spelling of URL and sending link or attachment of file by email. The phishing threat taxonomy model is experimented from the (1-4) as an ideal.

4. Phishing Methods Experiment

To find the rate of phishing attack method, the following equation is used for calculation:

$$\alpha_P = \left(\sum_{i=1}^{n} \frac{\alpha_{TiM}}{T_t \times \alpha_t} \times C \right) \times \left[\frac{C}{\sum_{s=1}^{s=20} \left\{ \sum_{i=1}^{m} \left(\sum_{i=1}^{n} \frac{C\alpha_{TiM}}{T_t \times \alpha_t} \right) \times X_\alpha \right\}} \right] \quad (1)$$

Let α_p denote the predicted rate (%) of a method used in predicted number of threats (T_t), α_{TiM} signifies the number of threats used in a method, assume that C is a constant number which is used to calculate percentage *(%)*, total number of threats can be calculated by T_t in our taxonomy model, number of threat used in a method, m is an arbitrary number and X_α is used as similar number of methods used in phishing threat, and s signifies number of methods used in our phishing taxonomy model. We have done the numerical experiment on the basis of our dataset by (1). Both numerical and graphical results are reported from (1) where the numerical results are shown in the following table I and graphical representation will be shown in section IV. The system structure of phishing method is the combination of three levels of method, which produces total phishing method (100%) used in our proposed model. In table I, we present the results of the experiment of categorizing the phishing methods in different levels on the basis of percentage of used method in multiple threats such as high, medium and low.

Through emails, phishers not only send URL in message body but also attach malicious file or image which can change the host file in PC or install some add-ons in the browser which automatically changes the IP addresses or redirects the page when typing the address of legitimate to a fake website. The first row in table I; shows the email method that is used 14.28% in phishing attack, the second row shows the abnormal DNS record which is 11.44% contributed by each threat. All other rows show the percentage of the total number of fields in that category sequentially, wrong or miss-spelled URLs and malicious files are 8.5% which can be categorized as high phishing method level. From the 5th to 8th row, methods using mid-level phishing methods using IDN, Popup, instant messages, SEO are mentioned which are sequentially 5.73%. Step by step other methods such as social engineering, double barrel attack, sending URL in SMS, using IP instead of DNS, M-it-M attack, Compromised host files, Trojan Horse used for URL redirection in host file, Session sniffing by phony pop up, Tab nabbing applied in a browser, voice Phishing applied by direct call to victim, wireless AP hacked by MitM attack, Compromised Server which categorizing in low method levels are 2.85%.

5. Phishing Origin Experiment

$$\beta_P = \left(\sum_{i=1}^{n} \frac{\beta_{TiO}}{T_t \times \beta_t} \times C \right) \times \left[\frac{C}{\sum_{u=1}^{u=8} \left\{ \sum_{i=1}^{m} \left(\sum_{i=1}^{n} \frac{C\beta_{TiO}}{T_t \times \beta_t} \right) \times Y_\beta \right\}} \right] \quad (2)$$

In (2), we denoted β_p as the predicted rate (%) of an origin used in predicted number of threats (T_t). The equation asks for five inputs, which are: number of threats used in an origin (β_{TiO}), total used origins in model (β_t), total number of threats (T_t), constant number (C) which is used to calculate percentage *(%)*, highest number of threats used in origins *(n)*, an arbitrary number (m) i.e. 1, 2, 3, ...100 and similar number of origins used in phishing threat (Y_β), number of origins used in our phishing taxonomy model (u) and one output which is β_P, signifies the predicted rate of origin used in predicted number of threats (T_t).

Three categories of origins are used in phishing attacks for which risk levels are: *High*, *Medium* and *Low*. The entries (2) are used for calculating phishing origin rate (%) which is shown in table II. The system structure is the combination of three levels of phishing threats origin, which produces total β_p*= 100%* used in our proposed model. The numerical results in table II shows that the website is 26.32% and human factor is 21.06% origins have much effect on the overall variation in the number of threat origin for any phishing attack. The amount of 15.79% origin is generated from browsers and 10.53% origin comes from malicious software. All other threat origins are 5.26% sequentially OS, malicious file, fake calls, insecure PCs, and wireless routers.

We used the following equation to calculate the rate (%) of origin used in phishing attack:

Phishing Method Experimental Results:

Method(α_i)	Total Number of Threats (T_i)												
	Fake Web.	Link manip.	Spear Ph.	Pharming	In session	Fake Web. Valid.	Fake popup	Phone Ph.	Malware Ph.	Search Engine	EEvil twins	DData Theft	**Methods (%)**
Email	3.04		2.80	2.79					2.95	2.70			14.28
DNS	3.02	2.88		2.64		2.90							11.44
URL	3.00	2.82	2.76										8.58
MaliciousFile		2.98		2.87							2.73		8.58
IDN	2.98	2.75											5.73
Popup					2.65		3.08						5.73
Instant messages	3.05									2.68			5.73
SEO								2.85		2.88			5.73
Social Engineering			2.85										2.85
Double barrel Attack			2.85										2.85
SMS			2.85										2.85
IP	2.85												2.85
M-i-M attack	2.85												2.85
Comp. host files				2.85									2.85

Trojan Horse				2.85									2.85
Session sniffing					2.85								2.85
Tabnabbing					2.85								2.85
Voice Phishing								2.85					2.85
ireless AP											2.85		2.85
Compromised Server												2.85	2.85

Phishing Origin Experimental Results

Priority Based Origin	**Total Number of Threats**												
No. of Origin	Fake Web.	Link manip.	Spear Ph.	Pharming	In session	Fake Web. Valid.	Fake popup	Phone Ph.	Malware Ph.	Search Engine	Evil twins	Data Theft	Origin (%)
Website	7.43	6.8				5.02	4.18			2.89			26.32
Human Factor	5.4	4.89						7.01		3.76			21.06
Browser		6.02	5.42		4.35								15.79
Software	4.27								6.26				10.53
OS				5.26									5.26
Malicious file			5.26										5.26
Fake calls								5.26					5.26
Insecure PC												5.26	5.26
Wireless router											5.26		5.26

6. Phishing Component Experiment

Phishing Component Experimental Results

Priority Based Threat Component	**Total Number of Threats**												
	Fake Web.	Link manip.	Spear Ph.	Pharming	In session	Fake Web. Valid.	Fake popup	Phone Ph.	Malware Ph.	Search Engine	Evil twins	Data Theft	Component (%)
Scripting languages (js, php, html, anchoring)	6.13	4.41	5.6	4.42	5.23	2.2	2.15		4.21	1.9		2.1	38.35
DNS		4.46	2.87	4.13									11.46
Email		2.21	5.56										7.77
Popup					2.11		5.66						7.77
Auto validation toolbar						3.85							3.85
Host file poisoning				3.85									3.85
Web browsers		3.85											3.85
Malicious USBs			3.85										3.85

Wireless Access Point											3.85		3.85
Telephone & VoIP								3.85					3.85
RAT			3.85										3.85
Attachments with file			3.85										3.85
File download									3.85				3.85

Phishing Target Experimental Results

Priority Based Threat Target	**Total Number of Threats**												
	Fake Web.	Link manip.	Spear Ph.	Pharming	In session	Fake Web. Valid.	Fake popup	Phone Ph.	Malware Ph.	Search Engine	Evil twins	DData Theft	Target (%)
User credentials (Account numbers, PIN etc.)	5.61		5.29		4.25	3.67		5.98		3.21	3.25	3.52	34.78
Click on URL/page to redirect to fake site	5.21	4.75				4.88	2.55						17.39
Host file	4.57						4.13						8.70

Email Attachment/link			4.89	3.8									8.69
SMTP			3.71	4.98									8.69
Human Asset									4.35				4.35
Exploiting browser vulnerabilities				4.35									4.35
DNS server table modification									4.35				4.35
Data theft				4.35									4.35
Take control of PC												4.35	4.35

There are various types of components used by social engineers to deceive people. We can easily calculate the percentage of a component by using the following equation:

$$\gamma_P = \left(\sum_{i=1}^{n} \frac{\gamma_{TiC} \times C}{T_t \times \gamma_t} \right) \times \left\{ \frac{C}{\sum_{v=1}^{v=13} \left(\sum_{i=1}^{m} \left(\sum_{i=1}^{n} \frac{C\gamma_{TiC}}{T_t \times \gamma_t} \right) \times Z_\gamma \right)} \right\} \quad (3)$$

Components of phishing threats have been derived (3) by γ_P to define predicted rate (%) of a component used in predicted number of threats. The number of threats used in a component is γ_{TiO}, C defines as constant number (100), total threat signifies by T_t, total component is represented by γ_t, n is used to denote the highest number of threat used in a component, m is any arbitrary number i.e. 1, 2, 3,....,100, v=1 to no. of component, and same number of component used in phishing threat is signified here by Z_γ. The table III shows each category of threat component in phishing taxonomy model.

The first row demonstrates the phishing components as scripting languages (*js, php, html, anchoring*) and the rate at which they are used by the phishers is 38.35%, the second row shows the abnormal *DNS* record which is 11.46% contributed by each threat component while the mid-level threat components *email* and *pop-up* have used 7.7%. All other rows show the percentage of the total number of components such as auto validation toolbar, host file poisoning, web browsers, malicious USBs, wireless access point, telephone & VoIP, RAT, attachments with file, file downloads are 8.5% which can be categorized as low level phishing components.

7. Phishing Target Experiment

Garera et al. showed that the blacklist URLs generally have significant percentages of IP addresses in the URL pathname.

$$\delta_P = \left\{ \sum_{i=1}^{n} \frac{\delta_{TiT} \times C}{T_t \times \delta_t} \right\} \times \left\{ \frac{C}{\sum_{w=1}^{w=10} \left(\sum_{i=1}^{m} \left(\sum_{i=1}^{n} \frac{C\delta_{TiT}}{T_t \times \delta_t} \right) \times Q_\delta \right)} \right\} \quad (4)$$

To calculate the rate of target used in phishing attack by (4) is: In (4) δ_P stands for predicted rate(%) of a target used in predicted number of threats, δ_{TiT} means number of threats

used in a target, C *is* given as constant number (100), total number of threats can be defined by T_t, the whole target of the phishers can be defined as δ, n is highest number of threat used in a target, m is also an arbitrary number i.e. 1, 2, 3, ...100, w=1 to no. of components and similar numbers of targets used in phishing threat signifies as Q_δ. In table IV, it is also apparent that the first row shows the phishers' main target which is to collect the user credentials (Account numbers, PIN, password etc.) which is 34.78%. The second row shows the click on URL/page to redirect to fake site is 17.39% contributed by each threat which are targeted at higher level. The mid-level target of phishers is to capture host file 8.70%, email attachment/link 8.69% and SMTP stands at 8.69%. All other rows show the percentage of the phishers' target sequentially; human asset, exploiting browser vulnerabilities, DNS server table modification, data theft and taking control of PC is 4.35%.

8. Discussion

The graphical representation has been demonstrated depending on the numerical experimental results. To demonstrate the phishing attack graphically, using all of the data crawled from data set [5-6], it has been found that 3,180 web sites out of 3,973 have been phishing by using the four equations used. From the result of calculation of phishing parameters, phishing threats can be grouped into 12 categories. Fig. 1 shows that a single method is used in various numbers of threats and experimented on twenty methods. Where the graph represents email, it is the main method which is used to steal user credentials. First four methods, *Email, DNS, URL and File,* have high risk level which is 42.88%. Each of the next four methods- *IDN, Popu, Internet Messaging, SEO*– have the same risks and belong to medium risk level, that is 22.92%. The rest of the methods have the same weight of risk and hence, the graph becomes a straight line and overall risk level is 34.20%.

Fig. 2 shows the origin of phishing attack, heterogeneous frequencies on the origin occupancy in most of the phishing threats. The high frequency of origin was set beforehand to form surveys and thus calculate the results using the equations mentioned before. When phishers use phishing attack, most of the attack's origins are the websites. Origin of phishing attack occupancy depends on average secondary phishers density *(i.e., total social engineers demand).* As a result, the origin of phishing attack curve becomes flat.

Figure 1: No. of threats used in a method to do phishing attack

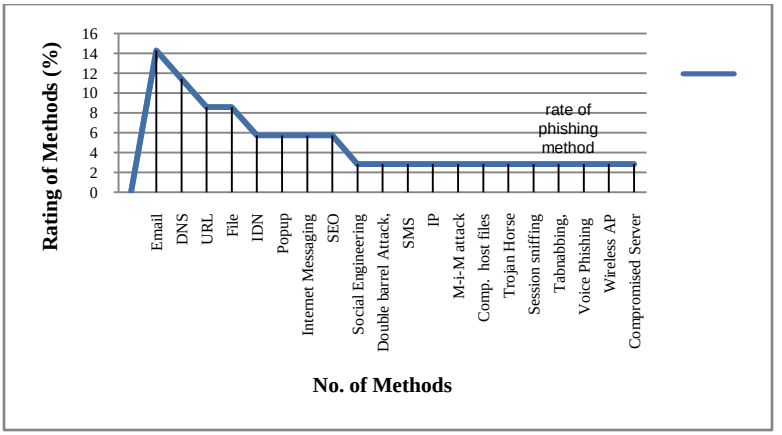

Figure 2: No. of threats used in an origin to do phishing attack

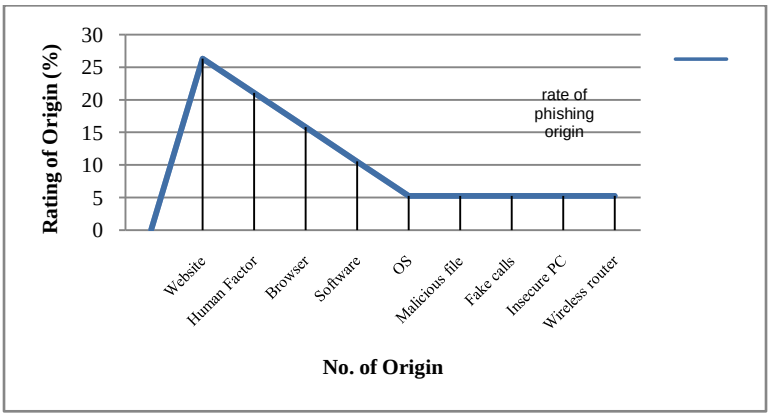

Fig. 3 details the attacks by thirteen phishing threats components of operation. A single component, scripting languages *(eg. js, php, html etc.)* are the most frequently used component having the high risk level which is 38.35%. The second most frequently used components have medium risk levels of 27% and then figure sharply steps down. The low risk level components (*eg. auto validation toolbar, host file poisoning, web browser setc.)* individually have the same weight of risk and the graph becomes a straight line and the accumulated risk levels are 34.65%.

In Fig.4, the frequency of phishing targets are increasing where phishers' main target is collecting user credentials to make financial loss of the victims. It also shows that the number of

target is very consistent, which is between 8.70% and 4.35%. The graphical curve and tabular model observations together with user credentials and page redirection experiment suggest that an annotation that enforces the phishing threat target behaviour for victim that perhaps will be substantially more applicable.

Figure 3: No. of threats used in a component to do phishing attack

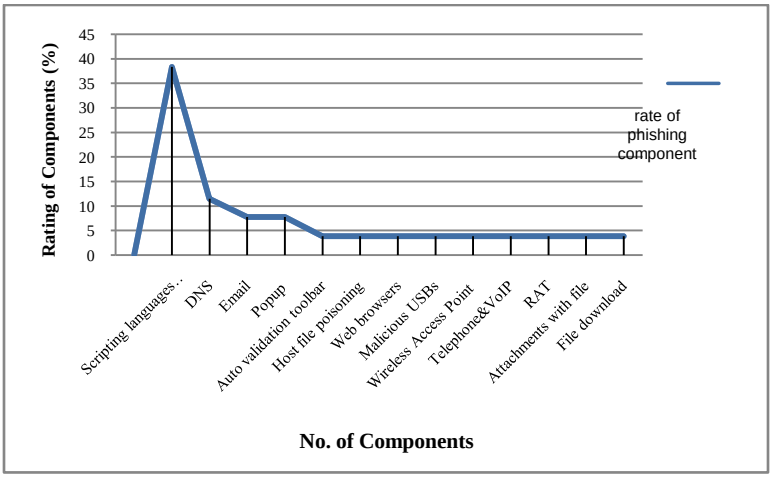

Figure 4: No. of threats used in a target to do phishing attack

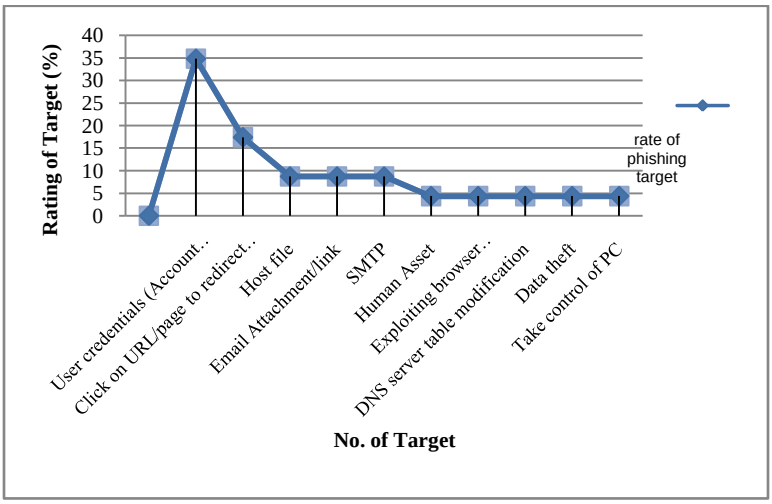

Table 5: Proposed Phishing Attack Detection Taxonomy Model

Threat	Method	Origin	Threat Comp.	Target
Fake website	URL Request Email message Instant messages DNS record Fake DNS	Software Website Human Factor	HTML java script PHP Cross-Site Scripting Malicious code	URL Fake Human Factor Redirecting to fake site
Link manipulation	Human Factor Sub domains Link anchoring IP instead of DNS Image file IDN	Long URL Sub-domain Anchor text Human Factor	Email Anchor text, web browsers DNS	Redirecting to fake site Click on fake site Deceived user Website.
Fake popup	Popup windows Capture Credentials	Website	HTML, Popup Java script	Redirect to Human
Fake website with	Registering similar DNS Man-in-the-middle	Website	HTML, Java script, Auto validation	Redirecting to User
Pharming	E-mails, upload file Compromised host files DNS Table	OS DNS	Host file poisoning HTML and Java script	SMTP Host file DNS Server
In session phishing	Phony popup messages, pop-up, Session,	Browser	popup software JavaScript	User credentials
Spear phishing	Email attachment, Hyperlink, Double barrel Attack, Social SMS phishing	Browser Malicious file	RAT, Scripting language, Attachments with (MS office, PDF	Email doc., Fake link Confidential

Phone phishing	Voice Phishing (Vishing)	Fake calls Human Factor	Telephone VoIP	Account numbers and PIN
Evil twins	Eavesdropping to AP, Bogus wireless access	RF, Router	Wireless Access Point (WAP)	Steal user credentials
Malware-Based	Email attachment, Downloadable file	Malicious software	Email, Malicious code	Exploiting browser
Search Engine	SEO	Fake web site	Fake anti- malware program	User credentials
Data Theft	Compromised Server	Insecure PC	Malicious code	Data theft

Other than technology, it is strongly encouraged for future victims of phishing attack to consider this result and the physiological existence of phishers. The above experimental results and discussion facilitate us to build the innovative phishing taxonomy model which is shown in table V. By using this model we can easily detect the behaviour and characteristics of phishing threat. This model is capable of detecting the parameters of phishing attacks which ultimately suggests the solutions to protect phishing attacks.

9. Conclusion

This paper looks at the phishing taxonomy holistically by examining various stakeholders and their counter measures, and by surveying experts' opinions about the current and future threats and calculating the percentages of the parameters of phishing taxonomy such as; origin, methods, components and targets by our proposed equations. The experiment led to four key findings on twelve threats and 624 ways to improve phishing attack detection. In the second experiment, the effectiveness of popular phishing equations to calculate methods, origins, components, targets which are used by major phishers have been displayed. Finally, graphical presentations of each parameter of taxonomy model have been exhibited for better understanding of phishing threat detection. By using this taxonomic model, a software is being developed which can efficiently detect the 99.99% phishing attacks which is still being tested before its official market launch.

References

Aaron, G. & Rasmussen, R. (2014). *Global Phishing Survey 2H2013: Trends and Domain Name Use*. APWG Internet Policy Committee. Retrieved from http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf.

Aburrous, M., Hossain, M. A., Thabatah, F., & Dahal, K. (2008, April). Intelligent phishing website detection system using fuzzy techniques. *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on* (pp. 1-6). IEEE.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behaviour*, *29*(3), 706-714.

Basnet, R., Mukkamala, S., & Sung, A. H. (2008). Detection of phishing attacks: A machine learning approach. *Soft Computing Applications in Industry* (pp. 373-383). Springer Berlin Heidelberg,

Bhati M., Khan R., (2012). Prevention Approach of Phishing on Different Websites. *International Journal of Engineering and Technology*,2(7).

Ding, Y., Pollacia, L., & Yang, S. (2015). Why Phishing Works: Project for an Information Security Capstone Course. *Information Systems Education Journal*, *13*(5), 71.

Gupta, S., & Kumaraguru, P. (2014, September). Emerging phishing trends and effectiveness of the anti-phishing landing page. *Electronic Crime Research (eCrime), 2014 APWG Symposium on* (pp. 36-47)

Hamid, I. R. A., & Abawajy, J. H. (2014). An approach for profiling phishing activities. *Computers & Security*, *45*, 27-41.

Li, B., Ruifeng, S., Xin, F., Xue, L., & Wei-hao, C. (2014, October). Emergent Challenges and IPDS for Anti-Phishing Attack. *IT Convergence and Security (ICITCS), 2014 International Conference on* (pp. 1-4). IEEE.

Phishing Activity Trends Report, 2nd Quarter 2014, APWG Retrieved from: http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf

Vijayalekshmi, S., & Rabara, S. A. (2010, December). Fending financial transaction from phishing attack. *Trends in Information Sciences & Computing (TISC), 2010* (pp. 171-175). IEEE.

Xiang, G., Hong, J., Rose, C. P., & Cranor, L. (2011). Cantina+: A feature-rich machine learning

framework for detecting phishing web sites. *ACM Transactions on Information and System Security (TISSEC)*, *14*(2), 21.

Xu, Z., Wang, H., & Jajodia, S. (2014, October). Gemini: An Emergency Line of Defence against Phishing Attacks. *Reliable Distributed Systems (SRDS), 2014 IEEE 33rd International Symposium on* (pp. 11-20).

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, S Mi Shing & Vishing: An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307.