Assessment of Spear Phishing User Experience and Awareness: An Evaluation Framework Model of Spear Phishing Exposure Level (SPEL) in the Namibian Financial Industry

Viktoria Shakela and Husin Jazri
Department of Computer Science
Namibia University of Science and Technology
Windhoek, Namibia
victoriashakela@gmail.com, hjazri@nust.na

***Abstract*— Social engineering has become a major threat to organisations' IT systems. Users are normally the weakest links in security chains and they put their organisations at risk of internet attacks through various social engineering tricks implemented by online criminals. One of the thriving electronic social engineering attacks that is increasingly targeting electronic banking systems and users is spear phishing attack. Consequently, this research assessed user experience and awareness by evaluating users' abilities to detect if a specific email is spear phishing. Moreover, the research proposes an evaluation framework for an effective assessment of the organisations' exposure level to spear phishing threat. In the SPEL evaluation framework, two information security frameworks (ISO27001:2013) and (NIST SP 800 -53) were applied to identify threat vital signs within the organisation, whereas the Protection Motivation Theory (PMT) theory was used in the identification of the user vulnerability signs.**

Keywords— user vulnerability, spear phishing, social engineering, SPEL, information security

I. INTRODUCTION

In the past few years, financial industry has started moving towards e-banking services. Therefore, electronic transactions are becoming popular than traditional methods of banking transactions. This can be attributed to the convenience of customers being able to bank electronically through the internet, anywhere and anytime. On the positive side, this has greatly created customers' satisfaction with banking services, but it has also attracted cyber-crimes and attacks from the internet. One of the rising types of attack implemented by cyber criminals is phishing. With reference to [1], phishing is any form of crime that unlawfully, and through social engineering, obtains data from victims for the attacker's benefit, over an electronic communication channel.

As noted recently, attackers are using more sophisticated attacks to improve the success rate in stealing data and breach IT systems' security. As most organisations become more aware in detecting bulk phishing emails and communications through detection techniques, antispam mechanisms and improved user awareness, phishers have made a major shift from bulk phishing to spear phishing attacks that have had serious consequences for victim organisations.

According to [2] definition, spear phishing is a targeted phishing attack as it is directed towards a specific organisation or individuals and its content is well customized for the targeted organisation or individuals as opposed to bulk phishing and spam mails. Furthermore, [3] states that spear phishing differs from phishing in that rather than targeting a large number of prospective victims, a specific business owner or employees are selected. The attack is tailored to enhance its perceived legitimacy. In this type of attack, the phisher learns and gathers information about the victim to allow him an opportunity of sending a convincing content email to the potential victim. As emphasised by [4], most organisations only ensure that their network layers are protected from attacks through implementation of security mechanisms such as firewalls, SSL certificates and Intrusion Prevention Systems (IPS). Nonetheless, organisation remain exposed to spear phishing if users are unable to detect targeted attacks because these attacks do not target the systems but rather the people that use the systems.

Most of the analysed terms and definitions about spear phishing derive their explanation from the process and technicality employed by spear phishers. For instance, [5] clarifies that spear phishing is an electronic communication targeted at an individual or an organisation to extract information that can be used to attack the communication line in such a way that the victim performs an action that enables the attacker to gain access to the system. A major distinctive factor between spear phishing and traditional bulk phishing is that a random hacker towards randomly selected victims initially performs bulk phishing, whereas, a hacker who is in possession of the potential victim's personal information mostly performs spear phishing and the communication is normally customized.

The latest Phishing Activity Trends Report released by [6] shows that attacks targeting consumers have remained at high levels, with hundreds of phishing websites established online every day to lure online users to become victims. A recent report from [7] also confirms that ninety-one (91%) percent of cyber-attacks suffered by businesses recently start with spear phishing. Furthermore, a report by [8] has placed Namibia in the top 10 countries with most online banking users being targeted by online criminals using different attack methods such as Banking Trojans and social engineering, which in most cases incorporates spear phishing techniques.

978-1-5386-9236-3/19/$31.00 ©2019 IEEE

The current statistics on spear phishing have shown an enormous increase in spear phishing incidences [9]. The report published by [10], highlights that targeted or spear phishing attacks and advanced persistent threats are the major security concerns among organisations that participated in the study.

The success of the spear phishing attacker mainly depends on the following conditions according to [11], the source must appear to be a known and trusted entity, the information within the attack message supports its validity and the request made by the attacker seems to have logical basis. A thorough analysis of all three conditions reveals user compromise rather than the system to execute an attack and hence the success rate of this type of attack can be attributed to the organisation's user awareness and experience upon receiving spear phishing attack related communication.

The present research focuses on assessing spear phishing threats within the financial industry of Namibia as well as evaluating the current organisational user experience and awareness in the banking industry. Moreover, the study explored factors that have influence on user susceptibility to spear phishing attacks. The study proposed spear phishing evaluation framework, derived from two theories concerning the attacker's perspective and the potential victim's perspective, to allow for a deep understanding and the breaking up of an attack into its core components and approaching each as a problem to be solved such that specific solutions are reached to prevent the attack. The focal point is assisting the process of framework development of reducing spear phishing attacks by firstly understanding how users interact with a spear phishing email.

II. Related Works

Studies done on understanding users' susceptibility to phishing related attacks used pre-defined factors that have likelihood of influencing users' response towards spear phishing. For instance [12] studied the participants' detection abilities based on individual's differences and culture. Their study results indicated that individuals' ability to detect spear phishing is more influenced by national culture as well information security awareness. In a more related study by [13] findings discovered that there exists a link between user vulnerability to spear phishing and personal characteristics such as dominance, steadiness and conscientiousness. Meanwhile, [14] examined the viability of Equal-Viability Signal Detection Theory (EVSDT) to evaluate users' detection ability of spear phishing. The research results suggest that EVSDT can be effective in monitoring and assessment of phishing detection education and training. However, their research participants performed poorly in detecting spear phishing, with only forty percent (40%) correct detections.

It is noted in [15] that lack of information literacy skills is the major reason why users fall victim to spear phishing. Nonetheless, studies such as [16][17] that explored user awareness in an effort to evaluate the effectiveness of awareness in mitigating phishing attacks has been found to have some significant methodological drawbacks. These studies included university students and staff that were placed in unrealistic situations where they played some roles and hence making it difficult for their results to be applied in an industrial setting.

III. Methodology

A. Research Design

To empirically study these propositions and with the exploratory nature of the study in consideration, a qualitative methodology was applied on an organisation in the financial industry. This study follows a deductive approach to a case study design, and as such, it urges the definition of questions and propositions in advance of data collection. A suitable method to obtain behavioural variables and the identification of relationships between variables is a survey research in which the researcher selects a sample of people and asks them questions relating to the issue of research as stated by [18].

B. Data Collection

In specific to this research, the survey questions were constructed so that the researcher could collect users' knowledge and awareness, as well as to explore the influential factors on users' vulnerability to spear phishing attacks. The study applied two (2) methods for identification of organisational and user vulnerabilities to the existing threats, namely, questionnaires and semi-structured interviews. A survey was done with 179 participants to assess how well they are prepared to deal with spear phishing threat signs. Semi-structured interviews were conducted with information security officials in the financial industry.

The online questionnaire was developed such that it is divided into two sections. Section one (1) collected users' awareness, knowledge and experiences of spear phishing attack. Furthermore, section one (1) consisted six (6) questions; each question illustrates an email sample and a question for the participants to classify the email. For each email sample, a participant could choose one out of three options ('bulk phishing', 'spear phishing' and 'legitimate email'). Section two (2) of the questionnaire was used to identify user vulnerability signs based on the following four (4) PMT theory constructs, Perceived Vulnerability (PV), Perceived Severity of Threat (PSOT), Self-Efficacy (SE) and Response Efficacy (RE).

IV. Proposed Framework Model

The framework adopts a chronological process strategy combined with a predictive formula to compute the SPEL of the case study organisation. The framework design proposes a collective approach of reducing spear phishing attack opportunities from two perspectives that are; threat source and Vulnerability to the threat sign. In doing so, it allows the projection of the attacker/threat perspective to the vulnerability perspectives and determining the attack opportunities that the motivated spear phisher can exploit in the absence of security mechanisms and the security behaviour of users.

A. Threat Derivation

The threat signs are derived from current surveys, literatures and reports. The threat signs are logically formulated based on two (2) information security frameworks (ISO27001:2013) [19] and the NIST SP 800-53 [20]. Moreover, the appropriate security requirements for each threat are outlined as a guide to an organisation in implementing the correct security measures against a specified threat sign.

B. *Vulnerability identification*

Determining the appropriate method to find out if there is a matching vulnerability to the captured threats in the organisation. This leads to formulation of vulnerability vital signs for each threat sign.

C. *Threat matching*

Each vulnerability identified is matched to the corresponding captured threat. Under this process, elimination is performed, in cases where a specific vulnerability does not match any threat or a specific threat does not match any vulnerability. A score for each vulnerability vital sign question is an input into the framework correlation process to enable computing of each threat exposure level.

D. *Correlation and elimination*

This includes scoring of vulnerabilities to determine the risk exposure level of the matching threat to determine the vulnerability exposure level to a given threat. For each vulnerability that is likely to be exploited by the matching threat and that can cause an individual or an organisation to fall victim to spear phishing, a value called Threat Exposure Level (TEL) is calculated as illustrated in (1)

$$TEL = VS/TS * 100\% \quad (1)$$

Where VS refers to the vulnerability score and TS is the threat sign value. Each of the vulnerability level scores is assigned a different weight determined by the vital signs scores which is used in the calculations of the TEL. None = zero (0), Low = one (1), Medium = two (2) and High = three (3). The exposure level is expressed as percentage.

E. *Categorisation*

The levels for the vulnerability score as compared to the correlated threat. A level zero is an indication that there is no vulnerability to the specified threat. Whereas a score of three (3) designates a high vulnerability to the specific threat which increases the threat exposure level.

F. *SPEL computing*

Once TEL for all vulnerabilities is calculated, the overall SPEL is calculated as in (2). Fig. 1 depicts the described SPEL framework model.

(accumulated TEL)/ (total threat signs)*100%. (2)

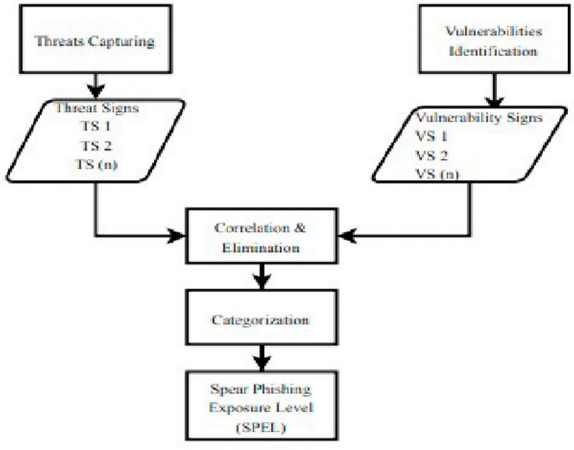

Fig. 1. SPEL framework model

V. RESULTS

A. *User experience and knowledge of spear phishing*

Out of 179 survey participants, four (4) failed to complete the classifications. Hence, their responses were excluded from the evaluation, resulting in 175 valid observations. The survey results indicate slightly good awareness of spear phishing threat among participants. The total correct classification responses (i.e. choosing 'legitimate' for emails that were received genuinely 'bulk' for spam emails and 'spear' for emails containing features of targeted attack emails) is 52%, in comparison to incorrect classification with 48%. Nevertheless, results suggest that users' knowledge to detect spear phishing needs to be improved. Further, result analysis per email shows inconsistency among participants to correctly identify spear phishing emails as presented in TABLE I.

TABLE I OVERALL PARTICIPANTS' EMAIL CLASSIFICATIONS

Email No.: Email type	**Participants classifications**	
	Correct classifications	***Incorrect classifications***
1: Bulk phishing	48%	52%
2: Spear phishing	67%	33%
3: Legitimate Email	42%	58%
4: Spear phishing	59%	41%
5: Spear phishing	51%	49%
6: Spear phishing	46%	54%

B. *SPEL model application*

To apply the proposed framework model, a case scenario sample was to assess the exposure level of disclosing confidential data such as bank account numbers and Private Identity Numbers (PIN) to an attacker through spear phishing techniques. Initially, the implementation process of that scenario was mapped to the model created through accurately projecting the threat signs and vulnerabilities that are necessary to successfully execute this attack.

Phase 1: Threat -> Vulnerability matching

Each vulnerability is matched to a corresponding threat sign or signs existing. The threat signs that match none or low vulnerabilities are less likely to be actioned into a successful spear phishing and hence they are none or low threat exposure level. In contrast, threat signs that match high vulnerability are more likely to be triggered into successful attack, hence they are high or medium threat exposure level. TABLE II illustrates an example with three captured threats to determine if there are matching vulnerabilities to these threats. Even though the study used twelve (12) threat signs in the model, complete threat -> vulnerability analysis are not displayed in this paper for space reasons.

TABLE II. THREAT -> VULNERABILITY ANALYSIS

Threat Sign	Vulnerability Sign Checklist
Email Spoofing	Does the organisation have tools to verify email source authenticity
Domain Spoofing	Are there mechanisms in place to detect spoofed URLS and domain authenticity
Identity Theft	Are there authentication methods that ensure that the identities of users, processes and devices are really who they claim to be

Phase 2: Correlation and Elimination

Vulnerabilities are interlinked in relation to threat and other security components that provide additional information about the threat in the organisation. This involves scoring of the threats and vulnerabilities to determine the risk exposure level of a given threat in correspondence to its projected vulnerability or to determine the vulnerability exposure level to a given threat, as illustrated with TABLE III.

TABLE III. CORRELATION

Exposure level	Vulnerability score	Threat value
67	2	3
100	3	3
33	1	3

Phase 3: Categorisation

The levels for the vulnerability score as compared to the correlated threat. A level zero is an indication that there is no vulnerability to the specified threat. Whereas a score of three (3) designates a high vulnerability to the specific threat which increases the threat exposure level. For instance in the given example, the model categorise one high threat, one medium threat and a low threat sign.

Phase 4: SPEL computing

SPEL for the three analysed vulnerabilities is computed as described in (2).

TABLE IV. SPEL RESULTS

Description	Value
Accumulated TEL	5
Total threat capture	9
SPEL	66.7%

VI. CONCLUSION

The study focused on measuring the awareness, knowledge and experience of end users on spear phishing and the results were presented. Nevertheless, the participants' knowledge to detect spear phishing prompted for the development of appropriate and focused mechanisms to improve the detection and classification of spear phishing attacks. The factors explored determined that PMT elements, especially Perceived Vulnerability (PV), have a potential of increasing users' detection of spear phishing and therefore it is recommended in the design of countermeasures aiming to increase user protective behaviour towards spear phishing. Through understanding the threat exposure level and users' vulnerability and behaviour to spear phishing, organisations can apply the proposed SPEL framework to assess and reduce spear phishing related threat signs.

ACKNOWLEDGMENT

The authors would like to offer special gratitude to Namibia University of Science and Technology (NUST) for the opportunity to conduct research and to publish the research work. In particular, the authors would like to thank Digital Forensics and Information Security (DFIS) cluster at NUST for their contribution to this research work.

A. Authors and Affiliations

1. Viktoria Shakela is a Master of Computer Science student at Namibia University of Science and Technology (NUST). She is a holder of Bachelor of Computer Science (Honours) in Information Security from the same university.

2. Husin Jazri is an Associate Proffessor at the faculty of Computing and informatics, NUST. He holds CISSP certification from the International Security Proffessional Certification Consortium (ISC)², the recipients of the Harold Tipton Lifetime Achievement Award in 2010 from the said Proffesional Association.

REFERENCES

[1] M. Khonji, Iraqi and A.Jones, "Mitigation of spear phishing attacks: A content-based authorship identification framework," in Proc. of the 2011 International Conference for Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates [Online]. Available: IEEE Xplore, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6148475. [Accessed: 31 March 2017]

[2] J. Aycock, "A Design for an anti-spear-phishing system" in Proc. of the Virus bulletin conference, 19-21 September 2007, Vienna, Austria [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.71.7778&rep=rep1&type=pdf. [Accessed: 03 May 2017]

[3] A. Hutchings, Theory and crime: Does it compute. PhD [Thesis (PhD Doctorate)]. Brisbane: Griffith Univ., 2013. [Online]. Available: Griffith Theses - Higher Degree by Research.

[4] J.Hong, "The state of phishing attack", Communication of the ACM, Vol.55, No.1, pp.74-81, 2012. [Online]. Available: ACM Digital Library, http://delivery.acm.org/10.1145/2070000/2063197/p74-hong.pdf [Accessed: 03 May 2017].

[5] M. Rouse, "Spear Phishing" Search Security, TechTarget, 2010. [Online]. Available: http://gauss.ececs.uc.edu/Courses/c6056/pdf/social-engineering-spear-phishing.pdf. [Accessed: 03 Dec 2016].

[6] Anti-Phishing Work Group, "Phishing activity trends report," July 3, 2018. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf. [Accessed: Nov. 14, 2018]

[7] TrendLabs APT Research Team, Spear phishing email: Most favored attack bait," 2012. [Online]. Available: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf. [Accessed: Nov. 14, 2018]

[8] M. Garnaeva, J. van der Wiel, D. Makrushin, A. Ivanov and Y. Namestnikov, 'Kaspersky security bulletin 2015. Overall statistics for 2015", Dec. 15, 2015. [Online]. Available: https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf. [Accessed: May 31, 2016].

[9] "Symantec, Internet security threat report," April 2016. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf. [Accessed: May 31, 2016].

[10] "Cisco 2017 Annual Cybersecurity Report," 2017. [Online]. Available: https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html. [Accessed: Feb.3, 2017].

[11] D. D. Caputo, SL. Pfleeger, J. D. Freeman and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," IEEE Security & Privacy, Vol.12, No.1, pp. 28-38. Jan-Feb 2014. [Online]. Available: IEEE Xplore, https://ieeexplore.ieee.org/document/6585241. [Accessed: Apr. 20, 2017]

[12] M. Butavicius, K. Parsons , M. Pattinson , A. McCormac , D. Calic and M. Lillie, "Understanding Susceptibility to Phishing Emails:Assessing the Impact of Individual Differences and Culture," in Proc. of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017), 28-30 November 2017, Adelaide, Australia. [Online]. Available: https://pdfs.semanticscholar.org/e098/5512826c150b243efe7cb35a514b21ce272c.pdf. [Accessed: 31 January 2018]

[13] C.Chuchuen, and P.Chanvarasuth, "Relationship between phishing techniques and user personality model of Bangkok internet users," ThaiScience, Vol.36, No.2, pp. 322 – 334. May 2015. [Online]. Available: http://www.thaiscience.info/Journals/Article/TKJS/10978275.pdf. [Accessed: Sept. 10, 2016]

[14] J. Martin, C. Dubé and M. D.Coovert, "Signal Detection Theory (SDT) Is Effective for Modeling User Behavior toward Phishing and Spear-Phishing Attacks," Human Factors: The Journal of the Human Factors and Ergonomics Society, Vol.60, No.8, pp.1179–1191. July 2018. [Online]. Available: Sage Journals, https://journals.sagepub.com/doi/10.1177/0018720818789818. [Accessed: Aug.31, 2018].

[15] J. E. Thomas, "Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks," International Journal of Business Management, Vol.12, No.3, pp 1-23. May 2018. [Online]. Available: https://ssrn.com/abstract=3171727. [Accessed: Aug. 31, 2018].

[16] K. Krombholz, H. Hobel, M. Huber and E. Weippl, "Advanced social engineering attacks," Journal of Information Security and Applications, Vol. 22,No.1, pp.113-122. June 2015. [Online]. Available: ScienceDirect, https://www.sciencedirect.com/science/article/pii/S2214212614001343. [Accessed: Sept. 10, 2016]

[17] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Lessons from a real world evaluation of anti-phishing training," in 2008 eCrime Researchers Summit, 15-16 October 2008, Atlanta, GA, USA. [Online]. Available: IEEE Xplore, https://ieeexplore.ieee.org/abstract/document/4696970. [Accessed: May 31, 2017]

[18] J.Rowley," Designing and Using Research Questionnaires", 2014, [Online]. Available: https://e-space.mmu.ac.uk/579515/1/Designing%20and%20using%20Research%20QuestionnairesREV18042013.pdf. [Accessed Dec. 01, 2017]

[19] ISO, "ISO/IEC 27001: 2013 Information technology Security techniques," [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed: Dec. 01, 2017].

[20] NIST, "SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf. [Accessed: Dec. 01, 2017].