International Journal of Engineering & Technology, 7 (4.29) (2018) 25-30

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

The Potential Factors Influencing Information Security Awareness on Phishing Attacks From Various Industries: A Systematic Literature Review (SLR)

Ayman Hasan Asfoor[1*], Fiza Abdul Rahim[2,3]

[1]*Department of Management of Information Technology, Jubail Industrial College, Saudi Arabia*
[2]*College of Computer Science and Information Technology, Universiti Tenaga Nasional, Malaysia*
[3]*Institute of Informatics and Computation in Energy, Universiti Tenaga Nasional, Malaysia*
**Corresponding author E-mail:asfour_a@jic.edu.sa*

Abstract

Phishing attack is one of the techniques used by attacker to get private information from Internet banking customers. This study will systematically analyse published research exploring factors that influencing information security awareness on phishing attacks. A total of 150 articles were used in our review a quality criterion was applied on this set of articles, a total of 20 articles were determined for further analysis, and successfully identified eleven factors as being either directly or indirectly related to awareness on phishing attacks. The factors are security concerns, user competence, computer literacy, self-efficacy, neuroticism, openness, response efficacy and years of PC usage. Moreover, studies have also identified the important role played by motivation. In this way, one could group factors relating to awareness on phishing attacks in three major groups including personality traits, motivation and individual differences. This review may be significant in providing useful information on how to understand users' susceptibility and vulnerability to phishing scams online.

Keywords: *Information security, Phishing, Security awareness*

1. Introduction

Given the fast-paced technological development and the incessant increase in cyber security threats, ignorance of information security issues can prove to be very costly. For instance, individuals who rely on internet banking for conducting most of their financial transactions are particularly vulnerable to threats such as trojans, malware, phishing, spyware, and keylogger software [1]. Among these cyber security threats, phishing is one of the most prominent methods of compromising one's Internet banking security.

It is worth mentioning that The Oxford English Dictionary defines phishing as "The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers." [21]. Thus, it appears that in this particular threat a scam email usually informs victims of an alleged security breach in their account, and subsequently requesting users to change their respective passwords [2]. In this particular instance, malicious emails normally impersonate a trustworthy financial organisation requesting account information, and when users actually respond to it by logging into the bogus site, attackers gain access to their bank account [3]. Moreover, it is quite interesting to notice that many victims of phishing end up never realising that they have actually been victims of phishing, and the vast majority of victims end up not even reported [4].

Over the past 10 years, there has been a substantial increase in deliberate attacks on users using deceptive techniques as means of carrying out electronic fraud in the form of phishing [5]. It follows that a considerable amount of research and scholarship has devoted its attention to find solutions regarding the best ways to protecting internet users from phishing attacks. Among these, one can identify technical solutions such as anti- phishing toolbars that connect to a database of blacklisted phishing websites [4]. One should note that phishing has business and consumers in the United States [6]. Thus, due to its prominence, phishing has become a major cyber security threat nowadays, and one of the ways in which to leverage security is through spreading awareness on this issue.

The aim of systematic literature review (SLR) in this study is to identify, assessing, interpreting and summarise all current information and available research about information security awareness (ISA) on phishing attacks in a comprehensive and unbiased manner. This is in order to draw more general conclusions regarding ISA on phishing attacks especially from individual studies. Moreover, it will also help in identifying the factors that influence the awareness of various industries regarding the information security awareness in phishing.

None SLR has been in identifying factors that influence ISA on phishing attacks. Therefore, it is needed to identify behavioural factors, which increase users' susceptibility to comply with bogus requests from phishing emails.Research Question
Population, Intervention, Comparison, Outcomes, and Context

(PICOC) structure of questions are shown in Table 1. The primary focus in this study was to understand and identify the factors that influence the potential factors influencing information security awareness on phishing attacks from various industries. In order to identify to what extent the information security on phishing attacks study has been conducted, this work investigates to answer the following primary research questions:

Table 1: Summary of PICOC

Population	Any organisation
Intervention	Information Security Awareness on Phishing Attacks
Comparison	None
Outcomes	Information Security Awareness on Phishing Attacks
Context	Review (s) of any published articles of information security awareness on phishing attacks within the domain of any applied case study setting in any organisation. No restriction on the type of study applied.

Based on the PICOC structure, the primary question of this study as follows:
What are the evidences of any information security awareness on phishing attacks studies conducted in any environment settings that investigated information security awareness effectiveness align with phishing attacks?

The study of SLR also aimed to answer the following secondary sub question: Sub question 1: What evidence is there regarding factors that affect information security awareness on phishing attacks, and which are the most effective factors? Sub question 2: How was the information security awareness on phishing attacks study has been conducted and being implemented in previous studies?

2. Review Method

The study adopts a SLR to outline the related factors. This review conforms to standard guidelines for conducting SLR of Information Systems Research, as prescribed by [7]. The review included only published articles conforming to the following criteria: (a) publications of original data concerning factors influencing awareness on information security in phishing attacks, (b) papers published between 2010 and 2017, (c) publications, which included both a quantitative and qualitative

design. In addition, the literature search was conducted using three databases: Science Direct, Google Scholar and IEEE Xplore. The keywords that were used in the search process included: (information security AND security awareness AND phishing AND systematic). A total of 20 articles were carefully selected based on three main criteria including;

(1) articles belonging to disciplines other than information security were immediately excluded,
(2) articles were selected only from the most credible and reputable sources, and
(3) articles were mainly aligned with European and North American research traditions within information security because these countries are most targeted by phishing attacks [45].

A structured approach was adopted as means of determining the source of relevant materials for review. In this way, the primary sources such as databases were given main preference. Data was reduced to manageable proportions in order to make the review feasible and in this way isolate journal articles, which were relevant to information security and suitable for further evaluation.

A total of 150 articles were specified based on the keywords search of its title and abstract: 10 articles were obtained from Science Direct, 70 articles were obtained from Google Scholar, 50 articles were obtained from IEEE Xplore, and 20 papers were obtained from Conferences. All articles were checked for duplication, resulting in 50 several articles. Thereafter, these articles were furthermore filtered by checking the content of their title and abstract. 100 articles that did not meet the chosen criteria were excluded accordingly. The remaining 60 articles were accessed for eligibility, and 20 articles that sufficiently provide information of its data source and used distinctive factors for prediction were selected for the review.

3. Findings

Based on our search from the digital libraries through the selection process, we identified three journals and two conferences in the information security awareness and phishing attacks fields as the baseline of our essential search. The first stage of our search process provided a total of 150 studies using "information security awareness" OR "awareness of cyber security" search term. The selection execution was composed by three stages as shown in Fig. 1.

In stage 2, we individually reviewed the papers based on their title, abstract and keyword of the remaining 150 articles were filtered and only 60 were chosen. By skimming the full text of the remaining 60 studies was tested in greater detail. Each of these studies was screened according to eligibility criteria and exclusion criteria before being accepted for the synthesis of evidence. Any duplicate studies were carefully checked to avoid redundancy. In final stages, a total of 20 articles were therefore included in the review.

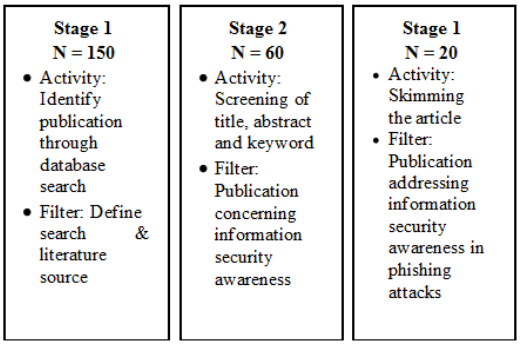

Fig. 1: Identifying relevant literature

2.1. Security Concerns

Security concerns is a reliable tool in predicting user's attitudes towards security awareness. A study conducted by [10] found that there is a lack of empirical studies on information security awareness, specifically when it comes to addressing issues relating to Internet banking among students in tertiary education. Their study had two key objectives including (a) to identify factors which potential influence awareness of information security issues for internet banking, (b) to examine the extent to what there is a link between identified factors and tertiary students' awareness on information security for internet banking. In their study, a questionnaire survey was used as the method for data collection. Results identified eight factors influencing awareness, computer literacy, regulatory literacy, security care, information support, social norm, recovery facility, and security concern.

In article [30], it addressed security concerns like opening of email attachments with potentiality of causing a phishing attack.

According to [4] the people have become more conversant with the security issues of information systems. The rise of the cloud computing technology has a different meaning to various people. It provides on-demand scalability of highly available and reliable pooled computing resources. Despite the benefits of cloud computing, it has brought security issues and concerns to different people and organizations.

2.2. Computer Literacy

Based on [10], the user's competence with information system challenges such as free Wi-Fi, email practices or passwords is also another factor that influences information security awareness in phishing attacks and another attribute is the individual differences which is made from a number of demographic and other variables. For example, someone who has high level of computer literacy and many years of usage, then the individual will be able to judge the level of threat coming from a phishing attack. The works of [5] in their literature review have found that the organizations have given the users using personal computers that may or may not support security best practices. The lack of computer literacy and awareness among the users regarding

security issues have been identified as a significant issue in the factors influencing security awareness.

2.3. Years of PC Usage

Much research devoted to investigate computer-based interactions, deceptive communication, and non-verbal deception has implicated it in the growing problem of cyber security [6]. For instance, in a recent study by [8], it was found that the vast majority of online users are still at high risk of becoming a victim of phishing attacks. The study was focused on identifying factors which influence user's susceptibility to phishing attacks. As the main task in the study, the respondents were required to distinguish phishing pages from genuine ones. It is interesting to discover that from the total number of participants, only a small minority (25%) attained a score over 75%, which clearly indicates the level of vulnerability that the average user is still exposed to falling victim to phishing attacks, but most importantly, results from the study has shown that years of PC usage and gender significantly impact detection rate of pop-up and phishing attacks.

According to [37], the usage of personal computer is said to be the weakest link in information system security. The home computers do not follow the security practices and the actions taken as in phishing compromise themselves. The survey looks at the factors that influence security decisions for the personal computer users.

2.4. Personality Traits

When it comes to understand the relationship between personality traits and phishing, the study conducted by [12] stands out quite conspicuously. The study examined the relationship between the Big Five personality traits and response patterns to a phishing email. In addition, the authors also examined the way in which these traits exert an impact upon users' Facebook-related behaviour such as privacy settings and posting of personal information.

Their study revealed that neuroticism was the personality trait which most correlated with responding to phishing emails. Similarly, they also found a strong correlation between gender and response to malicious emails. The identified factors can contribute to susceptibility to online security and privacy attacks as well as certain personality traits that might cause higher phishing vulnerability.

In studies [24, 25], the Big Five Framework helps in explaining the personality traits renders one vulnerable to phishing attacks and how they affect the behaviour of a person about their gender, race or age. The works of [35] advocate that the application of information technology does not always end up in improving the security. The human factors such as the personality traits play a significant role in the computer security as it can impact on the behavior. They argue information security behaviors are also mainly influenced by the perception of risk by individuals. The human factors are affected by the culture of the organization and the security environment in their occurrence.

2.5. User Competence

In study conducted by [34], user's competence was identified as one of the factors that may be critical in preventing an attack when a phisher uses free phishing kits including images, emails or web page codes to initiate their attacks. The article [39] has discovered that the security concerns depend on the users' expertise and stakeholders to prevent phishing attacks. The users need to be trained and e-security awareness made. These play an important role in law enforcement and the use of the recent security software and systems. For this system and software to function correctly, user competence is required.

2.6. Motivation

Another factor is the motivation, which made from constructs such as self-efficacy, the perceived level of severity, response severity and response efficacy. Indeed, the response and the reaction of the individual towards a phishing attack is determined from his or her ability to understand the nature of the threat but also on how he or she believes that is able to respond on this. Based on study conducted by [9], has found a motivation plays a major role in a variety of behaviours relating to internet security. The study based its assumptions upon Protection Motivation Theory (PMT) and administered a survey on a student sample (N=202), as means of assessing their behaviours concerning information security.

Results indicated that respondents' motivation to practice security is contingent upon the levels of perceived severity, self- efficacy, response costs, as well as response efficacy. In other words, students are highly motivated if they perceive that the aforementioned factors are high. In turn, the authors concluded that PMT is reliable to predict concerning individuals' attitudes towards information security. Article [41] advocates that the information technology has influenced the human life significantly. But the information security is a big concern for both the users and the organizations. The human aspect should be considered when dealing with information security. Different individuals are motivated by various factors that influence their security information awareness. The number of attacks is increasing due to the desire for financial and criminally motivated actions to gain access to personal and confidential information.

2.7. Individual Differences

It follows that a theoretical review of relevant literature conducted by [11] investigated both contextual factors and individual differences impacting the susceptibility to phishing attacks. Their review was mainly concerned with exploring literature relevant to factors, which can help reducing vulnerability and susceptibility to such malicious attacks. From this review, it emerged that individual differences seem to play a key role in both awareness and likelihood behaviour in the presence of a phishing attack from this review, it emerged that individual differences seem to play a key role in both awareness and likelihood behaviour in the presence of a phishing attack.

These factors will help in identifying the impacts of susceptibility to such forms of malicious attacks in online contexts. Article [31]

in their survey found that the predominant weakness in securing information systems properly is the individual users in a given organization. The individual users have differences that affect the behavioral information systems. The paper has researched on the approaches to understanding the hackers, how to improve the compliance of security and cross-cultural behavior.

2.8. Openness

Openness seemed to be associated with posting more personal information on Facebook, which in turn would lead users to be more vulnerable to phishing emails. In contrast, there was no link between respondents' estimates of being vulnerable to phishing attacks and actually being a victim of such malicious attack. In this respect, [12] argued that susceptibility to phishing may have nothing to do with lack of awareness. In this way, the authors concluded by stating that better understanding of personality traits is needed in order to better understand users' vulnerability and susceptibility to phishing attacks. According to the research conducted by [44], the phishing attacks have increased for the online computer users. The study focused on the factors that made the users respond to the phishing tacks. The research found that the people with high openness tend to post most of their information on social media platforms and are less strict to the privacy settings. This makes them more susceptible to the privacy attacks. The susceptibility to phishing is not always due to lack of awareness of the phishing risks. Understanding the traits that contribute to the vulnerability can help the users come up with methods the increase their privacy and security in the coming years.

2.9 Neuroticism

Their study revealed that neuroticism was the personality trait which most correlated with responding to phishing emails. Similarly, they also found a strong correlation between gender and response to malicious emails. The identified factors can contribute to susceptibility to online security and privacy attacks as well as certain personality traits that might cause higher phishing vulnerability. Neuroticism is having a long- term tendency of being in a negative state.

Works of [42] sought to know whether information security awareness message themes are more or less compelling for the various individuals based on their personality traits. The study considered five different message themes that included deterrence, molarity, regret, feedback and incentive and how they relate to the Big Five, Machiavellianism and social desirability. According to [43], neuroticism is the strongest predictor of social engineering. The research aimed at investigating how organizational and other individual factors shape other worker's intentions to resist social engineering. These deceive the users to undertake actions that could make a way to leak their information. The phishing attacks psychologically manipulate the users to reveal their confidential information.

2.10. Perceived Level of Severity

The computer users should be educated on the phishing methods as a way to combat these threats. If the computer users understand the impacts of the phishing attacks, they would be more careful when on the internet. The works of [38] developed a game to educate the computer users to secure themselves against the phishing attacks. If the users understand the severity level of the attacks, they will be more careful while posting their personal information on different online platforms.

2.11. Response Efficacy

These are the beliefs of a person to whether some given action steps will actually help avoid the phishing threats. The works of [6] aim at understanding the behavioral factors that increase the user's susceptibility to complying with phishing attacks and request for personal information. Some of the response actions are perceived by the computer users to protect them from phishing attacks.

2.12. Self-Efficacy

Based on other study [17] there are four mail groups of factors influencing information security behaviour in improving awareness are namely self-efficacy, intention to IT security practice, security practice-care behavior, and security practice-technology.

3. Discussion

This review has successfully identified eleven factors that could be classified as being either directly or indirectly related to awareness of phishing attacks (see Table 2).

Table 2: Summary of Potential Factors Influencing Information Security Awareness

Authors	Method Adopted	Factors
[8,6,37]	Quantitative	Gender, years of PC usage
[17]	Quantitative	Self-Efficacy
[38]	Mixed method	Perceived Level of Severity
[34,39]	Qualitative	User competence
[10,5]	Quantitative	Computer literacy
[12, 35] [24,25]	Quantitative	Personality traits
[15,16]	Applying the model	Knowledge, attitude, behaviour
[9,41]	Quantitative	Motivation
[42,43]	Mixed Method	Neuroticism
[12,44]	Mixed Method	Openness
[6]	Qualitative	Response Efficacy

Moreover, studies have also identified the important role played by motivation. In this way, one could group factors relating to awareness of phishing attacks in three major groups including (1) Personality Traits, (2) Motivation (3) Individual Differences [6] (See Fig.2).

When examining relevant literature, it seems as though that there are inherent differences between users when it comes to their level of awareness, as well as the way they respond and comply to thee phishers demands. But most importantly, personality traits such as openness and neuroticism also seem to be related to vulnerability to phishing.

From current findings, it would appear that the reasons why individuals become victims of phishing attacks is far more complex and multifaceted than previously anticipated. For example, openness into a something new is a critical factor. There are users who are open into something new, they may not be aware that there may be a threat, while there are users who are very hostile towards something new and therefore they will not be open on when it comes.

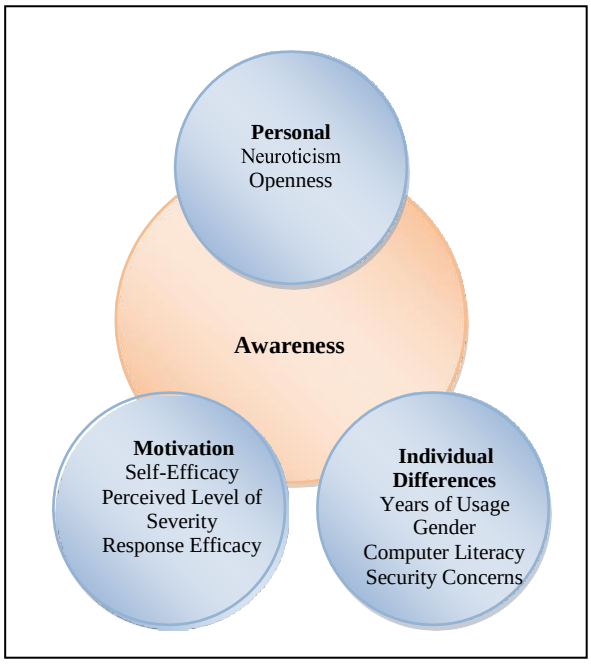

Fig. 2: The interrelationship between awareness, personality, motivation and individual differences

Another factor is the motivation, which made from constructs such as self-efficacy, the perceived level of severity, response severity and response efficacy. Indeed, the response and the reaction of the individual towards a phishing attack is determined from his or her ability to understand the nature of the threat but also on how he or she believes that is able to respond on this.

There are individuals who may appear to have high levels of self-efficacy and therefore they feel that even they are subject of a phishing attack they are ready to cope with this and to response appropriate, while the individual believes that he or she cannot cope with this, the most probable is to avoid getting any interference with something that may lead into a phishing attack.

Another attribute is the individual differences which is made from a number of demographic and other variables. For example, someone who has high level of computer literacy and many years of usage, then the individual will be able to judge the level of threat coming from a phishing attack.

For instance, when it comes to linking it to lack of awareness, it has been demonstrated that there is no link between perceived vulnerability and actually becoming a victim of phishing. Given these pattern of results one could argue that a combination of effective awareness campaigns, suitable cyber security training, together with automated tools could significantly reduce and prevent phishing attacks.

Thus, when it comes to developing a suitable theoretical model for understanding how the extent to what awareness (or indeed the lack of awareness) can contributed towards vulnerability one must perhaps adopt a holistic model as proposed by [11].

With respect, it would be sensible to realise that awareness, as a factor does not occur in isolation. As demonstrated in this review, awareness co-occurs with other factors. This makes establishing causal link between awareness and phishing quite difficult.

4. Conclusions and Future Work

Based on the discussion, it should be evident that the SLR identified important factors such as security concerns, user competence, computer literacy, personality traits, motivation, individual differences, self-efficacy, neuroticism, openness, response efficacy, years of PC usage. One must notice that the association between level of awareness of internet security issues and relevant factors was explored through quantitative studies.

The ever increasing usage of online services and the internet in general, has made internet security a topic of paramount importance. The take away message is that there are a variety of factors directly or indirectly linked to awareness of phishing attacks.

Moreover, as previously mentioned it is particularly difficult to establish a direct link between awareness and phishing, given the lack of correlational data linking the two. In addition, one must also take into account that awareness may co-occur with personality traits, individual differences, and gender to provide a multitude of behavioural responses to phishing and internet security related threats.

Therefore, future studies should thoroughly study the aforementioned factors together and, thus, adopt a holistic model to understanding users' susceptibility and vulnerability to phishing scams online. Finally, whilst acknowledging that awareness may not necessarily be directly linked to vulnerability, it is still sensible to assume that security against phishing scams can be enhanced though both educational programs about cyber security, as well as sharing important information regarding phishing attacks.

Acknowledgements

This work is supported by Start-Up Grant 2017 from Universiti Tenaga Nasional.

References

[1] Subsorn, P., & Limwiriyakul, S. (2011). A comparative analysis of the security of internet banking in Australia: A customer perspective. Paper presented at the *2nd International Cyber Resilience Conference, Perth, Western Australia*.
[2] Gan, C., Clemes, M., Limsombunchai, V. and Weng, A. (2006), "A logit analysis of electronic banking in New Zealand", *International Journal of Bank Marketing*, 24, 6, pp. 360-383.
[3] Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & information technology*, 32, 6, pp. 584-593
[4] IEC, Web Forum Tutorials, "Prepaid Services".
[4] Nagalingam, V., Narayana Samy, G., Ahmad, R., Maarop, N., & Ibrahim, R. (2015). Identifying the Level of User Awareness and Factors on Phishing Attempt Among Students. *Advanced Science Letters*, 21, 10, pp. 3243-3247.
[5] Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312.
[6] Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, 27, 1, pp. 273-303.
[7] Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, 37, 879 – 910.
[8] Iuga, C., Nurse, J. R., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, 6, 1, pp. 1-20.
[9] Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education*, 23, 4, 407.
[10] Ahmad Sobri Hashim & Saipunidzam Mahamad. (2017). Factors affecting awareness on information security in internet banking among Universiti Teknologi Petronas (UTP) students in Zulikha, J. & N. H. Zakaria (Eds.), *Proceedings of the 6th International Conference of Computing & Informatics* (pp 356-362). Sintok: School of Computing.
[11] Williams, E. J., Beardmore, A., & Joinson, A. N. (2017).

Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412-421.
[12] Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and facebook. arXiv preprint arXiv:1301. 7643.
[13] Kamal, S., & Shahibi, M. (2012). Information Security Awareness Amongst Academic Librarians. *Journal of Applied Sciences Research*, 8, 3, 1723-1735.
[14] Alseadoon, I., & Chan, T. (2012). Who is more susceptible to phishing emails?: A Saudi Arabian study. *23rd Australasian Conference on Information Systems.*
[15] Al-Alawi, A., & Al-Kandari, S. (2016). Evaluation of Information Systems Security wareness in Higher Education: An Empirical Study of Kuwait University. *Journal of Innovation & Business Best Practice*, 4 pages
[16] Allam, S., & Flowerday, S. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, pp. 56-65.
[17] Bojmaeh, H. (2015). The Main Factors Influencing Information Security Behavior. *International Journal of Science and Engineering Applications*, Vol. 4, 6.
[18] S. Alghathbar, B., & Nabi, S. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, pp. 10862- 10868.
[19] Kruger, H., & Flowerday, S. (2011). An assessment of the role of cultural factors in information security awareness. XeploreIEEE.
[20] N. Zanoon and N. Gharaibeh, (2013). The Impact of Customer Knowledge on the Security of E- Banking. *International Journal of Computer Science and Security (IJCSS)*, 7(2).
[21] Oxford Dictionary of English, Oxford University Press, Ed. Catherine Soanes, Angus Stevenson. ISBN 0-19-861347-4, ISBN 978-0-19-861347-3.
[22] Pham, H., Brennan, L., and Richardson, J. (2017). Review Of Behavioural Theories In Security Compliance And Research Challenges. In: *Information Science+ Information Technology Education Conference*. Ho Chi Minh City (Saigon), Vietnam: Information Technology Education Conference, p.14.
[23] Halevi, T., Memon, N., & Nov, O. (2015). Spear- Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN Electronic Journal*. doi:10.2139/ssrn.2544742.
[24] Veseli, I. (2017). Measuring the Effectiveness of Information Security Awareness Program. Masters. Gjøvik University College.
[25] Alhawari, S. (2014). Impact Evaluation of Customer Knowledge Process on Customer Knowledge Expansion. *Banking, Finance, and Accounting*, pp. 919-931. doi:10.4018/978-1-4666-6268-1.ch050.
[26] Al-Mayahi, I., & Mansoor, S. P. (2013). Information security culture assessment: Case study. In 2013 IEEE *Third Int. Conference on Information Science and Technology (ICIST)*, pp. 789–792. IEEE.
[27] Donahue, S. E. (2011). Assessing the impact that organizational culture has on enterprise information security incidents.
[28] Gebrasilase, T., & Lessa, L. (2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. *African Journal of Information System*, 3, 3, pp. 72–86.
[29] Puhakainen, P. (2017). a design theory for information security awareness. [online] Available at http://a design theory for information security awareness.
[30] Bauer, S. (2017). End User Information Security Awareness Programs for Improving Information Security in Banking Organizations: Preliminary Results from an Exploratory Study. [online] Association for Information Systems AIS Electronic Library. Available at: http://End User Information Security Awareness Programs for

[31] Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412-421. doi:10.1016/j.chb.2017.03.002.

[32] Veseli, I. (2017). Measuring the Effectiveness of Information Security Awareness Program. Masters. Gjøvik University College.

[33] AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49(2015), 567– 575.

[34] Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476– 486.

[35] Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2017). Human Factors and Information Security: Individual, Culture and Security Environment. [online] Available at: http://Human Factors and Information Security: Individual, Culture and Security Environment [Accessed 20 Dec. 2017].

[36] Drevin, L., Kruger, H. and Steyn, T. (2017). Value-Focused Assessment of Information Communication and Technology Security Awareness in an Academic Environment Lynette Drevin1, Hennie Kruger2 and Tjaart Steyn3. [online] Potchefstroom: North-West University South Africa, p.7. Available at: : https://www.researchgate.net/publication/220722398.

[37] Abraham, S. (2011). Information Security Behavior: Factors and Research Directions. In *AMCIS*.

[38] Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, 60, 185-197.

[39] Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, 30(8), 803- 814.

[40] Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33, 3, pp. 237-248.

[41] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, pp. 70-82.

[42] Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & Security*, 43, pp. 64-76.

[43] Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59, 26-44.

[44] Darwish, A., El Zarka, A., & Aloul, F. (2012, December). Towards understanding phishing victims' profile. In *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference* on (pp. 1-5). IEEE.

[45] Top 5 of Anything, (2018), https://top5ofanything.com/list/df54459c/ [Accessed: 1 May 2018].