Journal of Information System and Technology Management (JISTM)
Volume 5 Issue 16 (March 2020) PP. 01-14
DOI: 10.35631/JISTM.516001

Journal of Information System and Technology Management (JISTM)
Journal Website: http://jistm.com/
eISSN: 0128-1666

ASSESSMENT ON PHISHING AVOIDANCE BEHAVIOUR AMONG INTERNET BANKING USERS IN NIGERIA: A CONCEPTUAL MODEL

Fadare Olusolade Aribake[1], Zahurin Mat Aji[2]

[1] Faculty Art and Science, Universiti Utara Malaysia (UUM), Malaysia
Email: fadareolusolade@gmail.com
[2] Faculty Art and Science, Universiti Utara Malaysia (UUM), Malaysia

Article Info:

Article history:
Received date:07.01.2020
Revised date: 04.02.2020
Accepted date: 05.02.2020
Published date: 15.03.2020

To cite this document:

Aribake, F. O., & Mat Ali, Z. (2020). Assessment on Phishing Avoidance Behaviour among Internet Banking Users in Nigeria: A Conceptual Model. Journal of Information System and Technology Management, 5 (16), 01-14.

DOI: 10.35631/JISTM.516001.

Abstract:

Although, acceptance of Internet Banking (IB) has improved among banking customers due to the suitability it offers, there are quite few risks accompanying with its since it depends heavily towards the usage of Internet network, which has increased the chances of Phishing Attacks (PA). PA referred to as the most defiant of all information security threats and often perpetuated by conning user's information systems to inadvertently disclose their personal information or by modifying or deleting sensitive information and maliciously destructing and destroying users' resources Despite this huge enhancement, the ratio of usage has been relatively low, among IB users in Nigeria. This evidence indicates that there is an urgent requirement to investigate the factors behind the issue. Therefore, this study is conducted to develop a conceptual model based on Technology Threat Avoidance Theory (TTAT) to evaluate the PA among IB users in Nigeria and to enhance avoidance behaviour. This paper will present the initial investigation that leads to the development of the conceptual model. Researchers in this field can use the model in different populations and settings, and thus create an avenue in stopping the factors that contribute to the PA.

Keywords:

Technology Threat Avoidance Theory; Phishing Avoidance Behaviour; Internet Banking and Phishing Attacks

Introduction

The classy development of Internet Technologies (IT) application has brought significant impact on the way people conduct their way of life in the present-day scenario. The positive technological advantages coupled with incorporation of telecommunication technologies in the banking sector have subsidized the development of more flexible and user's friendly self-

service banking technologies to address quick and changing needs of banking clients (Kingshott, Sharma, & Chung, 2018; Paltayian, Georgiou, Gotzamani, & Andronikidis, 2017; George & Kumar, 2015). In the last 20 years, development of technology in business has impacted individual in a profound way due to its various benefits (Khedmatgozar & Shahnazi, 2018; Aribake, 2015; Yu, Balaji, & Khong, 2015). In addition, popularity and accessibility of the internet has been an important factor as it provides the backbone for IB services to take place (Angenu, Quansah & Okoe, 2015; Usman, 2018). However, growing availability of internet has led to increased availability of IB services (Aribake 2015). The scope of IB services comprises of Online Banking, Automated Teller Machines (ATM), Mobile Banking, and Short Messaging Service banking, POS and Mobile banking (Kavitha, 2017). Thus, banks worldwide have moved speedily to an era of technological changes whereby customers are exposed to Internet Banking (IB) platforms (Chauhan & Choudhary, 2016; Shaikh & Karjaluoto, 2016; Estrella-Ramon, Sánchez-Pérez, & Swinnen, 2016).

Although, acceptance of IB has improved among banking customers due to the suitability it offers, there are quite few risks accompanying with its since it depends heavily towards the usage of Internet network, which has increased the chances of online fraud and phishing attacks (Aboobucker & Bao, 2018; George, 2017). Phishing Attack (PA) is considered as the most defiant of all information security threats and often perpetuated by conning user's information systems to inadvertently disclose their personal information or by modifying or deleting sensitive information and maliciously destructing and destroying users' resources (Hameed & Arachchilage, 2018; Hameed & Arachchilage, 2016). However, phishing as at now still remains one of the ultimate online attacks towards banking institutions (Mridha, Nur, Saha, & Adnan, 2017), in which technical solutions have not been able to absolutely avert the raise of PA (He, Chan, & Guizani, 2015; Archchilage & Love, 2013; Arachchilage & Asanka, 2012; Anderson & Agarwal, 2010; Rhee, Kim & Ryuc, 2009). Hence, researchers tend to look into non-technical solutions such as; cheer phishing avoidance behaviour from users as a means of successfully combating such threats (Alghamdi, 2017; Arachchilage, Love, & Beznosov, 2016; Siponen, Pahnila & Mahmood, 2007; Pahnila, Siponen & Mahmood, 2007). The current lack of security shield amid most IB is conducive to PA (Alsayed & Bilgrami, 2017). Therefore, banking institutions must pay proper consideration in defending their user's information from unlawful groups/individuals who might entreaty after IB users account in a way of carrying-out deceitful happenings.

Literature Review

Phishing Attack (PA) threats is regarded as the most defiant of all information security threats which is habitually spread by defrauding user's information to unintentionally unveil their personal information via modifying, deleting sensitive information and unkindly destructing and abolishing users' resources (Hameed & Arachchilage, 2018). Likewise, phishing has severely grown-fully becoming a real threat to security globally and money-spinning criminal business model (Gupta, Singhal & Kapoor, 2016). Besides, PA is a technique known as social engineering used in misleading IB users to visit websites. Meanwhile the aim of such PA is that a hank (email or spam) is already directed across to IB uses for them to clasp the hank and automatically turn out becoming chase (Tewari, 2018). This kind of dishonesty makes the user to disclose their important data like their names, PIN, credit card facts and bank-account, whereas this taken data are used for the aim of swindling (Chauhan, 2017; Tewari, 2018). However, phishing remains one of the ultimate online attacks against financial institutions (Mridha, et al., 2017). Unfortunately, the recent lack of security guard amid most IB is conducive to PA threats (Alsayed, et al., 2017). Hence, there is need for banks to continually

Journal of Information System and Technology Management (JISTM)
Volume 5 Issue 16 (March 2020) PP. 01-14
DOI: 10.35631/JISTM.516001

ensure that IB channels are secure in taking into consideration the dynamic nature of technology and threats.

The statement from International Anti-Phishing Working Group (APWG), released that during the year 2016, it has shown the worst year in history for phishing scams having a total number of PA to be 1,220,523 indicating 65% increase over the number of attacks recorded in year 2015 (Pymnts, 2017). Furthermore, Figure1. shows total number of phish detected in year 2017 was 1 90,942, with the highest number occurring in August, which is normally one of the quietest months of the year (APWG, 2018; Chiew, Yong, & Tan, 2018). Figure 2. APWG, (2018) point at some notable increase in phishing that targeted towards payment, SAAS/webmail, financial institution, and cloud storage/file hosting as depict below.

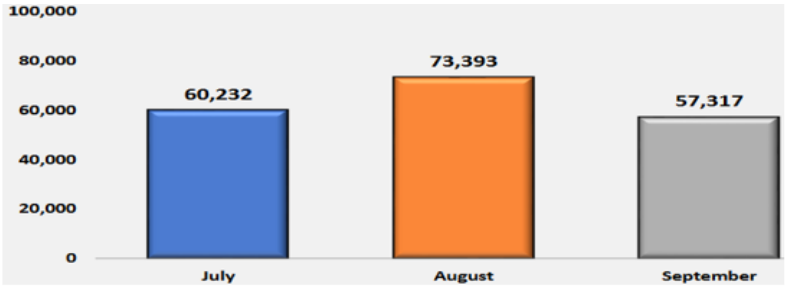

Figure 1: Unique Phishing Site Detected Sources: (APWG, 2018)

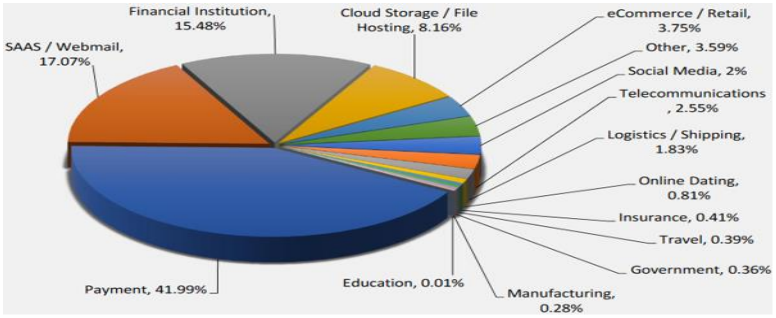

Figure 2: Statistics Showing Most Targeted Industry Sectors in year 2017 Sources: (APWG, 2018)

Moreover, Redmiles, Kross, and Mazurek, (2016) scrutinized user learning on security behaviour in work setting like banking sectors, even though little enquiry was carried-out to prove whether workplace behaviours translate to the home setting. Pursuing further, a large body of work has indeed focused on educating the efficiency of security behaviour (Redmiles, et al., 2016), in which it has touched via enlightening phishing education, by means of emerging more active cautions (Garg, Camp, Connelly, & Lorenzen-Huber, 2012; Arachchilage, et al., 2013), lessening security caution exhaustion (Bravo-Lillo, et al., 2013), and training users on how to generate a very durable password (Fujita, Yamada, Arimura, Ikeya, & Nishigaki, 2015; Schechter, & Bonneau, 2015). However, to aid wide scale improvement in user security, there is need to go beyond investigating the content of precise resource and educating these resources for individual behaviours like opinions and advice source that affect user's security (Rader & Wash, 2015). Thus, previous experience with some internet activities can have an influence on recent behaviour of users in terms of security.

Nevertheless, current literature on PA is found to be widespread with the lack of empirical evidence on its avoidance behaviour (Jansen, 2015). Concerning the trend of current studies on PA, it is impossible for banks to eliminate IB application from their platform (Jansen &

Leukfeldt, 2016). However, diverse web-browser have anti-phishing features in them, yet some users fails to take note of the cautionary, nor do not understand this cautionary or they deliberately disregard to the cautionary (Kuacharoen, 2017). This attack is targeted towards users who do not have knowledge around social engineering attacks and internet security (Gupta, et al., 2016; Leukfeldt's, 2014; Leukfeldt's, 2015). Therefore, there is a need to examine factors behind this issue, particularly among IB users.

Regarding the trend of recent studies in technology threat avoidance theory, the future behaviour of IB users cannot be predicted with certainty (Tewari, 2018). Meanwhile, previous literature is yet to reveal any attempt to structurally map out the relationship between system trust and its usage in the context of technology threat avoidance theory success. Moreover, banking system and specific banks are perceived as being a part of or even the origin of the financial crisis (van Esterik-Plasmeijer & van Raaij, 2017). However, the realistic effect of system trust in evaluating phishing avoidance behaviour success has not yet been clarified. This implies that the existing literature on technology threat avoidance behaviour lies in insufficient research in determining its predictors and thus requires further investigations.

Theoretical Background

Technology Threat Avoidance Theory (TTAT) is a theory proposed by Liang and Xue (2009) has widely been used in IS studies where this theory explains the importance of understanding information technology threat avoidance behaviour of users. The theory suggests that perceived effectiveness, perceived cost and self-efficacy constructs can influenced user's information technology threat awareness (Humaidi & Balakrishnan, 2013). Besides, the basic premise of TTAT is that when users perceive an IT threat, they are motivated to actively avoid the threat by taking safeguarding measures if the threat is thought to be avoidable (Manzano, 2012). Threat appraisal subsequently activates the coping appraisal in which the user assesses various coping mechanisms (Liang & Xue, 2009). The coping appraisal process evaluates one's ability to cope with and/or avert the perceived danger. TTAT suggests that in coping with a threat, an individual can thus take a proactive problem-solving approach to change the objective reality by carrying out an adaptive behaviour (Herath, et al., 2014). Liang and Xue (2010) tested their theory verifying the theoretical underpinnings and offering their model to explain technology threat avoidance behaviour. The original model includes perceived of vulnerability, severity, threat, safeguard effectiveness, safeguard costs, self-efficacy, avoidance motivation, and avoidance behaviour. A Google Scholar search of previous literature for TTAT yielded 88 results plus the two-original works (Carpenter, Young, Barrett & McLeod, 2019).

Liang and Xue (2009) analysed the associations in the model, by drawing from cybernetic theory and coping theory, TTAT delineates the avoidance behaviour as a dynamic positive feedback loop in which users go through two cognitive processes, threat appraisal and coping appraisal, to decide how to cope with IT threats. In the threat appraisal, Liang, and Xue, (2009) stressed that users will perceive an IT threat if they believe that they are susceptible to malicious IT and that the negative consequences are severe. The threat perception leads to coping appraisal, in which users assess the extent to which the IT threat can be made avoidable thru taking safeguarding measures based on perceived effectiveness, perceived costs and self-efficacy of applying the measure. TTAT posits that users are motivated to avoid malicious IT when they perceive a threat and believe that the threat is avoidable by taking safeguarding measures; if users believe that the threat cannot be fully avoided by taking safeguarding measures, they would engage in emotion-focused coping. Integrating process theory and variance theory, TTAT enhances our understanding of human behaviour under IT threats and makes an important contribution to IT security research and practice

DOI: 10.35631/JISTM.516001

Based on the preceding discussion, the study concludes that the entire constructs in TTAT are relevant to model the phishing avoidance behaviour among IB users in Nigeria. Liang and Xue (2010) found support for a positive association between one's beliefs about one's ability to implement a security safeguard and avoidance motivation, which makes perfect sense since individuals will be motivated to do something if they feel confident in their ability to do so (Carpenter, et al., 2019). However, many modification or improvement have been made on the model, but still very useful on avoidance behaviour. This shows that components of TTAT model are useful for modelling avoidance behaviour among IB users in Nigeria. In addition, the study also incorporates the system trust as the moderator since it has identified as a major issue that affect the users of IB (van Esterik-Plasmeijer, et al., 2017; Heider's 1958). Hence, there is still needed to also understand what motivate behaviour's by examining email contents or means to avoid clicking on suspicious website rather than installing or relying on automatic software (Dang-Pham & Pittayachawan, 2015).

Conceptual Model

The conceptual model for this study, as shown in Figure1 below, is based on the updated TTAT. It suggests that interaction between perceived severity and perceived vulnerability will significantly influences perceived threat. Likewise, interaction between procedural knowledge and conceptual knowledge will significantly influences self-efficacy. At the second level perceived threat and self-efficacy will significantly influence the avoidance motivation. In the same manner, the initial avoidance motivation should lead to more avoidance behaviour on phishing attack. As a result of these avoidance motivation and avoidance behaviour, that will further lead to improvement of TTAT (moderated by system trust of the IB user). At the same time, the users IB system trust is also expected to moderate the relationship between avoidance motivation and phishing avoidance behaviour. The antecedent of this conceptual model will be thoroughly discussed in the following subsections.

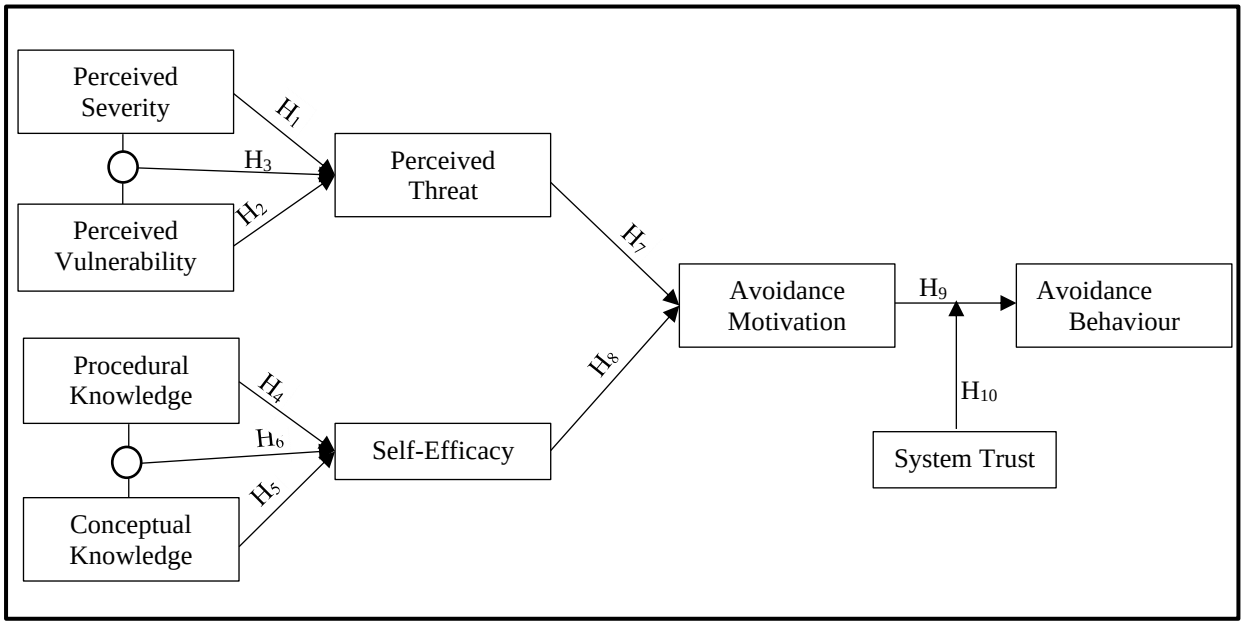

Figure 1: The Conceptual Model of Phishing Avoidance Behaviour among Internet Banking Users in Nigeria

Perceived Threat

Technology alone is insufficient to address critical IT security challenges. To date, there has been little work published on the human aspect of people per-forming security checks and

protecting themselves from various attacks which are imperative to cope up with cyber-threats such as phishing attacks (Arachchilage, Love & Beznosov, 2016; Alsharnouby, Alaca & Chiasson, 2015; Arachchilage & Love, 2014; Arachchilage & Cole, 2011). Consistent with TTAT (Liang & Xue, 2009), users' IT threat avoidance behaviour is determined by avoidance motivation, which, in turn, is affected by perceived threat. Perceived threat is influenced by perceived severity and susceptibility. Perceived threat is also influenced by the combination of perceived severity and susceptibility. Perception of a threat is likely to be affected by susceptibility, severity, and motivation, and evaluation of secure behaviour is likely to be affected by costs, benefits, and control (Davinson & Sillence, 2010). Once a threat is perceived and secure behaviour is chosen the user must also know when to conduct it. There is little evidence to indicate a predetermined sequence of events that must occur to successfully promote secure behaviour, or which factors need to be satisfied before others come into play. However, even if users are sufficiently motivated, feel susceptible, and perceive severe consequences it does not necessarily change their behaviour. Therefore, perceived susceptibility will be focused upon initially, as it is reasonable to assume this factor will increase concerns and motivation to act, which must be satisfied before a change in behaviour is even considered (Davinson, et al., 2010).

Self-Efficacy

Self-efficacy is defined as individuals' confidence in taking the safeguard measure. This is an important determinant of avoidance motivation. Previous research has revealed that individuals are more motivated to perform IT security related behaviours as the level of their self-efficacy increases (Kaiser, 1974; Ng, Kankanhalli & Xu, 2009; Woon, Tan & Low 2005). Self-efficacy has a co-relation with knowledge (Baral & Arachchilage, 2019; Hu, 2010; Hsu, Ju, Yen, & Chang, 2007). For example, when users are knowledgeable of avoiding phishing threats, they are more confident to take relevant actions to thwart phishing. The main objective of knowledge management is to support creation, transfer, and application of knowledge in a context (Alavi & Leidner, 2001; Hsu et al., 2007; Pfeffer & Sutton, 1999). For example, developing a software tool to create an awareness of cyber threats in the organisational context. It has been shown that the concept of self-efficacy has been applied to knowledge management in many contexts (Alavi & Leidner, 2001; Hsu et al., 2007). McCormick (1997) has stated that knowledge can be influenced by learning procedural and conceptual knowledge associated with technological activities. Plant (1994) has stated that procedural knowledge is remarkably close to the idea of ''know how'' and the conceptual knowledge is ''know that''. Furthermore, he explained that such conceptual knowledge allows us to explain why, hence the distinction of ''know how'' and ''know why'' (Arachchilage, Love & Scott, 2012). Additionally, McCormick (1997) argued that the two ideas of conceptual and procedural knowledge are frequently seen as separate, with their relationship being ignored. Therefore, we propose that both procedural and conceptual knowledge as well as its interaction effect significantly affect on self-efficacy, which contributes to enhance computer users' phishing threat avoidance behaviour.

The proposed model describes users' IT threat avoidance behaviour is determined by avoidance motivation, which, in turn, is affected by self-efficacy. Self-efficacy is influenced by procedural knowledge and conceptual knowledge. Therefore, user-centred security educational tools should consider the user SEF factor that will directly motivate them to perceive threat while working on cyber-space to avoid PA (Arachchilage, Love & Scott, 2012). According to authors in (Arachchilage, et al., 2017), it is essential to build threat perception in user so that they will motivate themselves to combat PA through their avoidance behaviour. Therefore, inter-relationship of CK and PK is the idea to 'know-how-to-it-by-knowing-that'. Young,

Carpenter and McLeod, (2016) found that severity significantly related to threat but that neither susceptibility to threat nor the interaction of severity and susceptibility on threat was significant. Chen and Zahedi (2016) reported the associations of susceptibility and severity significantly related to threat but did not test the interaction of susceptibility and severity. Finally, Bujang and Hussin (2012) suggested a modified full model that did not contain the interaction between susceptibility and severity hypothesized in the Liang and Xu (2009) original TTAT model. However, Bujang and Hussin (2012) did not empirically test their newly proposed model.

Avoidance Motivation

According to Liang and Xue, (2010) defines avoidance motivation as the behavioural intention to use a given security safeguard. This definition is important as it is a well-established notion that behavioural intentions are often a good predictor of actual behaviour (Verkijika, 2018). This view has been widely supported in the information security literature, a reason why many existing information security studies focus only on understanding user intentions to engage in different forms of information security behaviours (Dang-Pham, et al., 2015; Ifinedo, 2012; Menard, Warkentin & Lowry, 2018; Tsai et al., 2016; Vance, Siponen, & Pahnila, 2012). Nevertheless, while intentions might be a good predictor of behaviour, several researchers (Liang & Xue, 2010; Siponen et al., 2014; Thompson et al., 2017; Verkijika, 2019) have emphasized the need to examine actual behaviours to better understand how well security intentions translate to behaviours. Consequently, models for understanding security intentions are encouraged to extend and examine the link between intentions and actual security behaviours (Thompson, McGill & Wang, 2017). The expected positive influence of security intentions on security behaviours has been supported both in the organization (Siponen et al., 2014) and personal computing domains (Thompson et al., 2017; Verkijika, 2018), including online phishing threat avoidance behaviours (Arachchilage & Love, 2014).

Avoidance Behaviour

Up until now, most of IS studies have been conducted around the technology acceptance theory. Of course, it is very important to check the factors determining the acceptance of IT in using the IT. However, the acceptance behaviour is not the only thing in using IT. The attitude of trying to avoid IT may be a part of that behaviour. Accordingly, it would be quite meaningful to look into the IT threat-avoidance behaviour. Basically, the avoidance and acceptance behaviours are two different situations and the technology acceptance theory is not complete although it is important to understand the IT threat-avoidance behaviour of users (Rhoa & Yub, 2011). Since there are not many studies related to the IT threat, TTAT has expanded the theory by synthesizing various references in the fields of psychology, health care, risk analysis and information system.

In order to explain the behaviour of IT users that tries to avoid the threat of malicious information technologies, Liang and Xue (2009) have proposed the technology threat avoidance theory (TTAT). He mentioned that TTAT as a dynamic and positive feedback loop could explain about the avoidance behaviour through the cybernetic theory and coping theory. Here, users go through two cognitive processes and this is the coping appraisal that determines how to cope with the IT threat appraisal and IT threat. If users are aware of a malicious IT and consider it seriously as a negative result, they will perceive the IT threat. The threat awareness may draw a coping judgment and users may appraise the level that the IT threat can be avoided through the safeguarding measures such as perceived cost and self-efficacy (Rhoa, et al., 2011). When users judge that the IT threat can be avoided by the safeguarding measures, they may take a problem-focused coping measure; and when the IT threat could not be avoided

completely, they may take an emotion-focused coping measure (Rhoa, et al., 2011). The validity of TTAT starts with the assumption that the avoidance and acceptance behaviours of people are different in the qualitative perspective. This difference suggests the need of TTAT development. Humans inherently try to avoid a negative stimulus and tend to get closer to a positive stimulus (James 1890; Pavlov 1927; Skinner 1953). The stimulus in the IT environment refers to various information technologies.

System Trust

In the context of phishing avoidance behaviour, system trust is considered as one of the factors that possibly influence the use of a particular system like e-banking or financial institution. The issue of system trust has previously been recognized by previous researchers, particularly in the field of IB (van Esterik-Plasmeijer, et al., 2017; Nor & Pearson, 2015). For instance, the case study by van Esterik-Plasmeijer, et al. (2017) found that system trust is the expectation that the banking system and banks in general, in a specific country or internationally, will keep explicitly or implicitly made promises and behave in a favourable or, at least, not unfavourable way for the customer. Ever since the last century, the task of IB users has rapidly grown and the complaints on lack of system trust has become common among them (Hurley, Gong & Wagar, 2014; Järvinen, 2014; Shim, Serido & Tang, 2013). Considering this, future research on IB should include factor of system trust, as they believed that it would extend the explanation from the existing literature.

Model Validation

In order to realize the factors that potentially significant for the assessment of phishing avoidance behaviour among IB users, two technique of obtaining and validation are applied in this present study. Initially the literature review is conducted to search for the relevant factors connected to phishing avoidance behaviour, as discussed in the previous section. These selected factors were then given to the experts for confirmation on the appropriateness and suitability to be used on the model. In order to ensure validity of this procedure, the current study has chosen the experts based on two criteria. First, the lecturers should have seven years of teaching experience as the minimum requirement to be appointed as experts (Berliner, 2004). This criterion is important to the current study as the selected experts will review and determine the significance of the proposed factors from the perspective of the lecturers. Second, the experts in e-banking system should have at least three years of experience in the particular system (Svilar & Zupančič, 2016). As for the current study, this criterion will ensure that the experts are familiar with the phishing avoidance behaviour especially in term of the system, information and service quality. Therefore, the experts were selected based on their experience as lecturers (over seven years) and experience in dealing with phishing avoidance behaviour over three years. The findings of the expert review are shown in Table1.

Conclusion

The study seeks to contribute some understandings on how the new Conceptual Model that is developed based on the TTAT can predict the phishing avoidance behaviour among IB users in Nigeria. It is usable for researchers in information system and e-banking that interested in investigating the factors that contribute to the success of phishing avoidance behaviour in other setting and population. In conclusion, the study aims to fill the gap as none of the existing studies to the knowledge of the researcher provides the determinants on phishing avoidance behaviour. The successful implementation of system trust relies on its ability to meet the users' requirement and expectation, while at the same time provide a secured environment for its users. Thus, the outcome of the study will provide the guidelines for Nigerian banks especially

service providers to spot the weaknesses in the current practice on IB phishing avoidance behaviour.

Table 1: (Model Validation by the Experts)

Factor	Suggested by	Expert Review
Perceived Severity	(Ifinedo, 2012; Workman et al., 2008; Woon et al. 2005)	All expert rate factor to be a very significant one
Perceived Vulnerability	(Siponen et al., 2014; Ifinedo, 2012; Woon et al., 2005)	All the expert rate factor to be a very significant one
Procedural Knowledge	(Misra, et al., 2017; Arachchilage, et al., 2017; Arachchilage &Love, 2014)	All the expert rate factor to be a very significant one
Conceptual Knowledge	(Misra, et al., 2017; Arachchilage, et al., 2017; Arachchilage &Love, 2014)	All the expert rate factor to be a very significant one
Perceived Threat	(Samhan, 2017; Liang & Xue, 2010)	All the expert rate factor to be a very significant one
Self-Efficacy	(Arachchilage, et al., 2017; Arachchilage, et al., 2014)	All the expert rate factor to be a very significant one
Avoidance Motivation	(Arachchilage, et al., 2014; Liang, et al., 2009)	All the expert rate factor to be a very significant one
Avoidance Behaviour	(Arachchilage, et al., 2014; Liang, et al., 2009)	All the expert rate factor to be a very significant one
System Trust	(Li & Yeh, 2010)	All the expert rate factor to be a very significant one

Reference

Aboobucker, I., & Bao, Y. (2018). What Obstruct Customer Acceptance of Internet Banking? Security and Privacy, Risk, Trust and Website Usability and the Role of Moderators. The Journal of High Technology Management Research, 29(1), 109-123.

Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. MIS quarterly, 107-136.

Alghamdi, H. (2017). Can Phishing Education Enable Users To Recognize Phishing Attacks?

Alsayed, A., & Bilgrami, A. (2017). E-banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities. Int. J. Of Emerg. Techn. and Adv. Activ, 7(1), 109-115.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: user strategies for combating phishing attacks. International Journal.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioural intentions. MIS quarterly, 34(3), 613-643.

Angenu, B. B., Quansah, F., & Okoe, A. F. (2015). Determinants of Online Banking Adoption among Ghanaian University Students. Journal of Service Science and Management, 8(02), 183.

APWG, (2018). Phishing Activity Trends Report. https://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf

Arachchilage, N. A. G., & Cole, M. (2011). Design a mobile game for home computer users to prevent from "phishing attacks", Information Society (i-Society), 27-29June 2011(pp. 485e489). al of Human-Computer Studies, 82,69e82.

Arachchilage, G., & Asanka, N. (2012). Security awareness of computer users: A Game based learning approach (Doctoral dissertation, Brunel University, School of Information Systems, Computing and Mathematics).

Arachchilage, N. A. G., & Love, S. (2013). A Game Design Framework for Avoiding Phishing Attacks. Computers in Human Behavior, 29(3), 706-714.

Arachchilage, N. A. G., & Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. Computers in Human Behaviour, 38, 304-312

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing Threat Avoidance Behaviour: An Empirical Investigation. Computers in Human Behavior, 60, 185-197

Arachchilage, N., Love, S., & Scott, M. (2012). Designing a Mobile Game to Teach Conceptual Knowledge of Avoiding' Phishing Attacks'. International Journal for e-Learning Security, 2(1), 127-132.

Aribake, F. O. (2015). Impact of ICT tools for Combating Cyber Crime in Nigeria Online Banking: A Conceptual Review. International Journal of Trade, Economics and Finance, 6(5), 272.

Baral, G., & Arachchilage, N. A. G. (2019). Building Confidence not to be Phished Through a Gamified Approach: Conceptualising User's Self-Efficacy in Phishing Threat Avoidance Behaviour. In 2019 Cybersecurity and Cyberforensics Conference (CCC) (pp. 102-110). IEEE.

Bravo-Lillo, C., Komanduri, S., Cranor, L. F., Reeder, R. W., Sleeper, M., Downs, J., & Schechter, S. (2013). Your Attention Please: Designing Security-Decision UIs to make Genuine Risks Harder to Ignore. In Proceedings of the Ninth Symposium on Usable Privacy and Security (p. 6). ACM.

Bujang, Y. R., & Hussin, H. (2012). Investigating Email users Behaviour against Spam: A Proposed Theoretical Framework. Journal of Internet and e-Business Studies, 2012, 1.

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining Technology Threat Avoidance Theory. Communications of the Association for Information Systems, 44(1), 22.

Chauhan, V., & Choudhary, V. (2016). E-Banking Services in India: A Broad-Brush Survey of Indian Banks. IUP Journal of Bank Management, 15(1).

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and Behaviour's: Polycontextual Contrasts Between the United States and China. Mis Quarterly, 40(1), 205-222.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A Survey of Phishing Attacks: their types, Vectors and Technical Approaches. Expert Systems with Applications.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing Intention to Avoid Malware AcrossContexts in a BYOD-Enabled Australian University: A Protection Motivation Theory Approach. Computers & Security, 48, 281-297.

Davinson, N., & Sillence, E. (2010). It Won't Happen to me: Promoting Secure Behaviour Among Internet Users. Computers in Human Behavior, 26(6), 1739-1747.

Estrella-Ramon, A., Sánchez-Pérez, M., & Swinnen, G. (2016). How Customers' Offline Experience Affects the Adoption of Online Banking. Internet Research, 26(5), 1072-1092.

Fujita, M., Yamada, M., Arimura, S., Ikeya, Y., & Nishigaki, M. (2015). An Attempt toMemorize Strong Passwords while Playing Games. In 2015 18th International Conference on Network-Based Information Systems (NBiS) (pp. 264-268). IEEE.

Garg, V., Camp, L. J., Connelly, K., & Lorenzen-Huber, L. (2012). Risk Communication

Design: Video vs. Text. In International Symposium on Privacy Enhancing Technologies Symposium (pp. 279-298). Springer, Berlin, Heidelberg.

George, A. (2017). Precautions for Safe Use of Internet Banking: Scale Development and Validation. IIM Kozhikode Society & Management Review, 6(2), 186-195.

George, A., & Kumar, G. G. (2015). Validation of a Scale for Measuring Problems in Internet Banking and their Effect on Customer Satisfaction. Vision, 19(4), 312-323.

Gupta, S., Singhal, A., & Kapoor, A. (2016). A Literature Survey on Social Engineering Attacks: Phishing Attack. In Computing, Communication and Automation (ICCCA), 2016 International Conference on (pp. 537-540). IEEE.

Hameed, M. A., & Arachchilage, N. A. G. (2018). Understanding the influence of Individual's Self-efficacy for Information Systems Security Innovation Adoption: A Systematic Literature Review. arXiv preprint arXiv:1809.10890.

Hameed, M. A., & Arachchilage, N. A. G. (2016). A Model for the Adoption Process of Information System Security Innovations in Organisations: A Theoretical Perspective. In: The Proceeding of the 27th Australasian Conference on Information Systems, arxiv.org/abs/1609.07911.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security Servicesas Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service. Information Systems Journal, 24(1), 61-84.

Heider, F. (1958). The psychology of interpersonal relations. New York: John Wiley & Sons Ltd.

He, D., Chan, S., & Guizani, M. (2015). Mobile Application Security: Malware Threats and Defences. IEEE Wireless Communications, 22(1), 138-144.

Hu, M. L. (2010). Discovering culinary competency: An innovative approach. Journal of Hospitality, Leisure, Sports and Tourism Education (Pre-2012), 9(1), 65.

Humaidi, N., & Balakrishnan, V. (2013). Exploratory Factor Analysis of User's Compliance Behaviour Towards Health Information System's Security. Journal of Health & Medical Informatics, 4(2), 2-9.

Hurley, R.F., Gong, X. and Wagar, A. (2014), "Understanding the Loss of Trust in Large Banks", International Journal of Bank Marketing, Vol. 32 No. 5, pp. 348-366.

Hsu, M. H., Ju, T. L., Yen, C. H., & Chang, C. M. (2007). Knowledge sharing behaviour in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. International journal of human-computer studies, 65(2), 153-169.

Ifinedo P. (2012). Understanding Information Systems Security Policy compliance: An Integration of the Theory of Planned Behaviour and the Protection Motivation Theory. Computer Security, 31(1), 83–95. http://dx.doi.org/10.1016/j.cose.2011.10.007.

James, W. (1890), The Principles of Psychology, New York: Henry Holt & Co.

Jansen, J. (2015). Studying Safe Online Banking Behaviour: A Protection Motivation Theory Approach. In HAISA (pp. 120-130).

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. International Journal of Cyber Criminology, 10(1), 79.

Järvinen, R.A. (2014), "Consumer Trust in Banking Relationships in Europe", International Journal of Bank Marketing, Vol. 32 No. 6, pp. 551-566.

Kaiser, H. F. (1974). An index of factorial simplicity, Psychometrika.7.

Kavitha, S. (2017). 'Factors Influencing Satisfaction on E-banking',AIMS International Journal of Management, 11(2), pp. 103-115.

Khedmatgozar, H. R., & Shahnazi, A. (2018). The role of dimensions of perceived risk in adoption of corporate internet banking by customers in Iran. Electronic Commerce Research, 18(2), 389-412.

Kingshott, R. P., Sharma, P., & Chung, H. F. (2018). The Impact of Relational Versus Technological Resources on E-Loyalty: A Comparative Study between Local, National and Foreign Branded Banks. Industrial Marketing Management.

Kuacharoen, P. (2017). An Anti-Phishing Password Authentication Protocol. IJ Network Security, 19(5), 711-719.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), 551–555.

Leukfeldt, E. R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factor and possibilities for situational crime prevention. International Journal of Advanced Studies in Computer Science and Engineering, 4(5), 26–32.

Li, Y. M., & Yeh, Y. S. (2010). Increasing Trust in Mobile Commerce through Design Aesthetics. Computers in Human Behaviour, 26(4), 673-684.

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS quarterly, 71-90.

Manzano, D. L. (2012). The cybercitizen dimension: A Quantitative Study using a Threat Avoidance Perspective (Doctoral Dissertation, Capella University).

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination. Computers & Security, 75, 147–166

McCormick, R. (1997). Conceptual and Procedural Knowledge. International Journal of Technology and Design Education, 7(1-2), 141-159.

Misra, G., Arachchilage, N. A. G., & Berkovsky, S. (2017). Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. arXiv preprint arXiv:1710.06064.

Mridha, M. F., Nur, K., Saha, A. K., & Adnan, M. A. (2017). A New Approach to Enhance

Internet Banking Security. International Journal of Computer Applications, 160(8).Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying Users' Computer Security

Behaviour: A Health Belief Perspective. Decision Support System, 46(4), 815–825.Nor, K. M., & Pearson, J. M. (2015). The influence of trust on internet banking acceptance.

The Journal of Internet Banking and Commerce, 2007.Pahnila, S., Siponen. M., & Mahmood M.A. (2007). Employee's Behavior Towards IS Security

Policy Compliance," In: The Proceedings of 40th Hawaii International Conference on System Sciences, 1561.

Paltayian, G., Georgiou, A. C., Gotzamani, K., & Andronikidis, A. (2017). Combining Quality Management Tools with Quantitative Approaches to Improve e-Banking Operations. In Global Conference on Services Management (GLOSERV 2017) (p. 273).

Pavlov, I. (1927), Conditioned Reflexes: An investigation into the Physiological Activity of the Cortex, New York: Dover.

Plant, M. (1994). "How is Science Useful to Technology," Design and Technology in the Secondary Curriculum: A Book of Readings, The Open University, Milton Keynes, pp. 96–108, 1994.

Rader, E., & Wash, R. (2015). Identifying Patterns in Informal Sources of Security Information. Journal of Cybersecurity, 1(1), 121-144.

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2016). How I Learned to be Secure: A Census-Representative Survey of Security Advice Sources and behaviour. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 666-677). ACM.

Rhee, H., Kim, C., & Ryuc, Y, C. (2009). Self-efficacy in Information Security: Its Influence on End Users' Information Security Practice Behaviour. Computers & Security, 28, 816-826.

Rhoa, H., & Yub, I. (2011). The impact of information technology threat avoidance factors on avoidance behaviour of user. Dep. Bus. Manag. Sunc. Natl. Univ.

Samhan, B. (2017). Security Behaviours of Healthcare Providers using HIT Outside of Work: A Technology Threat Avoidance Perspective. In Information and Communication Systems (ICICS), 2017 8th International Conference on (pp. 342-347). IEEE.

Shaikh, A. A., & Karjaluoto, H. (2016). On Some Misconceptions Concerning Digital Banking and Alternative Delivery Channels. International Journal of E-Business Research (IJEBR), 12(3), 1-16.

Schechter, S., & Bonneau, J. (2015). Learning Assigned Secrets for Unlocking Mobile Devices. In Eleventh Symposium on Usable Privacy and Security (SOUPS 2015) (pp. 277-295).

Shim, S., Serido, J. and Tang, C. (2013), "After the Global Financial Crash: Individual Factors Differentiating Young Adult Consumers' Trust in Banks and Financial Institutions", Journal of Retailing and Consumer Services, Vol. 20 No. 1, pp. 26-33.

Siponen, M. T., Pahnila, S., & Mahmood, A. (2007). Employees' Adherence to Information Security Policies: An Empirical Study. In: The Proceedings of the International Federation for Information Processing IFIP SEC, Conference.

Skinner, B.F. (1953), Science and Human Behavior, New York: Macmillan.

Svilar, A., & Zupančič, J. (2016). User experience with security elements in internet and mobile banking. Organizacija, 49(4), 251-260.

Tewari, A. (2018). Detection and Classification of Spam and Phishing Emails.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security Begins at Home": Determinants of Home Computer and Mobile Device Security Behaviour. Computers & Security, 70, 376-391.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding Online Safety Behaviours: A Protection Motivation Theory Perspective. Computers & Security, 59, 138-150.

Usman, A. K. (2018). An Investigation into the Critical Success Factors for E-Banking Frauds Prevention in Nigeria (Doctoral dissertation, University of Central Lancashire).

van Esterik-Plasmeijer, P. W., & van Raaij, W. F. (2017). Banking System Trust, Bank Trust, and Bank Loyalty. International Journal of Bank Marketing, 35(1), 97-111.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3-4), 190-198.

Verkijika, S. F. (2018). Understanding smartphone security behaviours: An extension of the protection motivation theory with anticipated regret. Computers & Security, 77, 860-870.

Woon, I., Tan, G. W., Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. In International Conference on Information Systems (pp. 367–380). Las Vegas, NV.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. Computers in Human Behaviour, 24(6), 2799-2816.

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware Avoidance Motivations and Behaviours: A Technology Threat Avoidance Replication. AIS Transactions on Replication Research, 2(8), 1-17.

Yu, P. L., Balaji, M. S., & Khong, K. W. (2015). Building Trust in Internet Banking: a Trustworthiness Perspective. Industrial Management & Data Systems, 115(2), 235-252.

About the Authors

Fadare Olusolade Aribake she is currently a PhD student at the Universiti Utara Malaysia in Information Technology. She received her master's degree from same University in Information Communication Technology. Her primary research interests include behavioural and users' aspects of systems security including acceptance/rejection of security technologies, cybercrime, motivations for engaging in risky online behaviour, and online deception. She is also interested in information privacy, technology adoption/continuance behaviour's, and inter-organizational benefits/effects of information systems. She has published in the Journal of Internet Banking & Commerce, **Journal of Computer Engineering & Technology,** Journal of Information System & Technology Management, **International Journal of Advanced Research in Engineering & Technology** and International Journal of Trade Economics &Finance.

Zahurin Mat Aji currently a lecturer at the school of computing Universiti Utara Malaysia. She received her PhD in Information Technology from Universiti Utara Malaysia. And her master's in information system from Leeds University, United Kingdom in 1995. Her primary research interest includes community information, rural ICT development, ICT policy and strategy and management information system.