Journal of Computer Engineering and Technology (JCET)
Volume 4, Issue 01, January - June 2020, pp. 1-17, Article ID: JCET_4_01_001
Available online at http://www.iaeme.com/jcet/issues.asp?JType=JCET&VType=4&IType=1
Journal Impact Factor (2020): 4.6119 (Calculated by GISI) www.jifactor.com
ISSN Print: 2347-3908 and ISSN Online: 2347-3916
© **IAEME** Publication

MODELLING THE PHISHING AVOIDANCE BEHAVIOUR AMONG INTERNET BANKING USERS IN NIGERIA: THE INITIAL INVESTIGATION

Fadare Olusolade Aribake*
PhD Student in Information Technology
School of Computing, Awang Had Salleh College of Art & Sciences
University Utara Malaysia (UUM), 06010, Sintok, Kedah Malaysia

Dr. Zahurin Mat Aji
Lecturer, School of Computing,
Awang Had Salleh College of Art & Sciences
University Utara Malaysia (UUM), 06010, Sintok, Kedah Malaysia

*Corresponding Author Email : fadareolusolade@gmail.com

ABSTRACT

The positive usage of Internet Technology advantage had inspired the banking sector in Nigeria to invest in digitalizing the banking platform, which has been a move towards the usage of IB for financial services; however, such move also implies an increase opportunity for Phishing Attacks (PA). 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) and Modified TTAT to evaluate the PA among IB users in Nigeria and to enhance avoidance behaviour. As the study is still in the early stage, this paper will present the initial investigation that leads to the development of the conceptual model, including the background of the study, literature review and research methodology that the study wishes to employ. Finally, this study seeks to contribute some understandings on how the new Conceptual Model can predict the success of phishing avoidance behaviour among Nigerian IB users.

Key words: Technology Threat Avoidance Theory; Modified TTAT, Phishing Attacks, Phishing Avoidance Behaviour and Internet Banking

Cite this Article: Fadare Olusolade Aribake and Zahurin Mat Aji, Modelling the Phishing Avoidance Behaviour among Internet Banking Users in Nigeria: The Initial Investigation, *Journal of Computer Engineering and Technology* 4(1), 2020, pp. 1-17.
http://www.iaeme.com/JCET/issues.asp?JType=JCET&VType=4&IType=1

1. INTRODUCTION

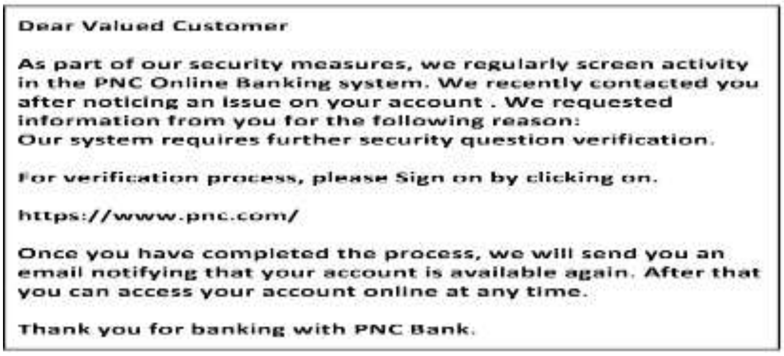
The classy development of Internet Technologies (IT) application has brought significant impact on the way people conduct their way of life in the present-day scenario. The usage of Internet technologies application has brought significant impact on the way people conduct life in the present-day scenario for enhancement of business performance which has evolved around the world (Khedmatgozar & Shahnazi, 2018). Besides, IB regarded as a radical technological innovation comprising a potential in changing the structure and nature of banking via speeding up its communication effects and transaction efficiency for its users (Sánchez-Torres, Canada, Sandoval & Alzate, 2018). Acceptance of IB has improved among banking customers due to the suitability it offers, there are quite few risks accompanying with its use since it depends heavily towards the opening of Internet network, which has increased the chances of online fraud and phishing attacks (Aboobucker & Bao, 2018; George, 2017). Phishing Attack (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 (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). Moreover, researchers are going in support for non-technical solutions such as; cheer phishing avoidance behaviour from users as a means of successfully combating towards PA (Alghamdi, 2017; Arachchilage, Love, & Beznosov, 2016). Unfortunately, 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.

2. LITERATURE REVIEW

2.1. Phishing Avoidance Behaviour

Phishing signifies a key form of online financial and identity theft that is unsafe to computer users, in which its goal is to steal subtle data like password, username's, and IB financial detail from its victims (Arachchilage, et al., 2016; Tambe Ebot, 2017). Here criminals generate a replica of a prevailing websites page to deceive victims for them to submit their personal details (Hatunic-Webster, 2017). 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 the cautionary (Kuacharoen, 2017). This attack is targeted towards users who do not have knowledge around social engineering attacks and internet security (Gupta, Singhal, & Kapoor, 2016). Figure1. displays a sample of phishing email that feigns to be from PNC bank asking users to sign in via clicking on the link displays by the bank URL (Kuacharoen, 2017). Although, the acts of clicking on phishing links are always like all phishing victims, just their reason for clicking are differs because they are affected by different traits like online behaviour, prior security knowledge and experience that disturb individual behaviour in diverse ways (Tambe Ebot, 2017). Once the victim clicks on such link, the phishing site comes up, and the users who has an account with the bank sign into untrusted site as instructed in the email, this makes the user to have given out his/her details mistakenly to the phisher (Kuacharoen, 2017; Ghosh, Li, & Yang, 2018).

In addition, phishing attacks has turn-out to become more classy overtime, whereby attackers taught of the techniques which are more active and alter their tactics accordingly (Chaudhary, 2016; Alghamdi, 2017). Besides, those working towards the stop of phishing do have less evidence than the attackers on how users respond to countless kinds of attacks. Also, preceding research has discovered that technology only is unsatisfactory to guarantee serious IT security problems (Arachchilage, et al., 2016). Meanwhile, there exist some work on end-user's behaviour in performing security and preventing users from attacks like phishing (Arachilchlage et al., 2014; Arachilchlage et al., 2016). Several claims by some security and usability experts that users' education towards security do not work, there is proof that well designed user security education can be active in the actual world (Arachilchlage et al., 2014; Arachilchlage et al., 2016). 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.



Dear Valued Customer

As part of our security measures, we regularly screen activity in the PNC Online Banking system. We recently contacted you after noticing an issue on your account . We requested information from you for the following reason:
Our system requires further security question verification.

For verification process, please Sign on by clicking on.

https://www.pnc.com/

Once you have completed the process, we will send you an email notifying that your account is available again. After that you can access your account online at any time.

Thank you for banking with PNC Bank.

Figure 1: An Example of Phishing Email (Kuacharoen, 2017)

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 (Jansen, 2015).

Furthermore, Tsai, Huang, Liu, Tsaur and Lin, (2010) clarified on the dynamic nature of technology and IB presents unique security challenges require novel solutions. Although, acceptance rate of IB has improved among banking customers due to the suitability it offers (Usman, 2018), some researchers emphasised on quite few risks accompanying with its since it depends heavily towards the usage of Internet network, which has increase the frequency towards PA threats, online fraud and cyberattacks as part of the challenges in securing IB services (Usman, 2018; Aboobucker, et al., 2018). The recent lack of security guard amid most IB is conducive to PA threats (Alsayed, et al., 2017). However, phishing at remains one of the ultimate online attacks against banking institutions (Mridha, et al., 2017). Hence, IB user's need to be cautions in their behaviour to avert PA. 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.

2.2. Technology Threat Avoidance Theory (TTAT) and Modified (TTAT)

Countless theories and models related to IS usage have been introduced including Technology Threat Avoidance Theory (TTAT) a theory proposed by (Liang & Xue 2009) and the Modified Theory of (TTAT) proposed by (Arachchilage & Love 2014). TTAT 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).

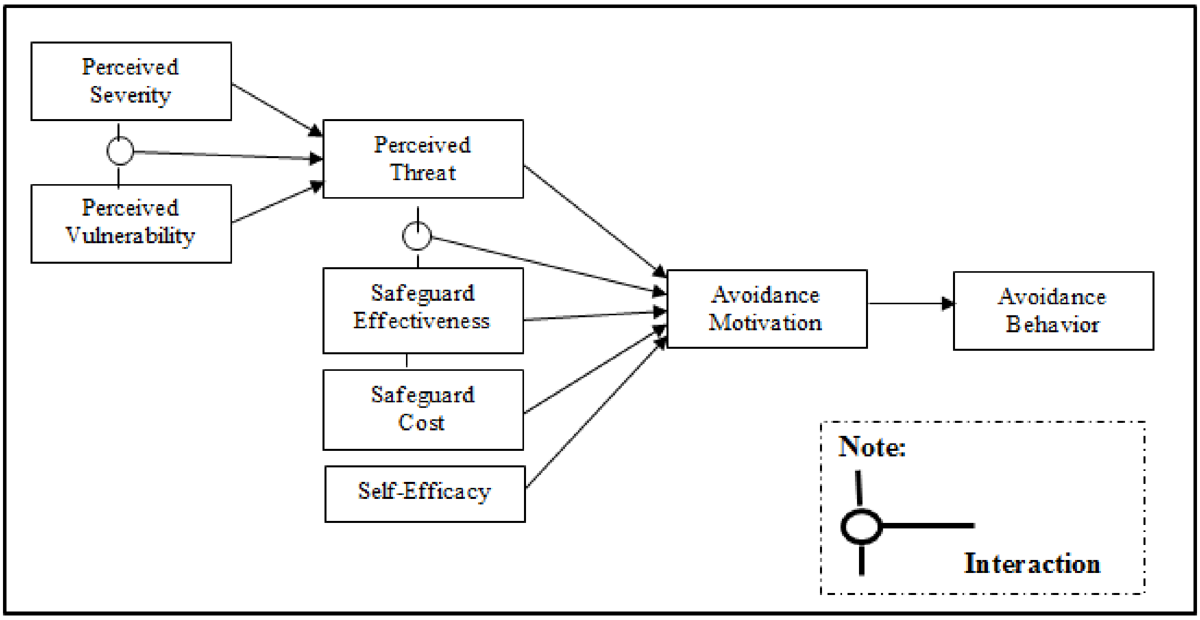


Figure 2: Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2010)

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.

Modified model of TTAT as propounded and validated by Arachchilage and Love (2014) to include relevant factors such as; conceptual or procedural knowledge and their roles in influencing end-user's self-efficacy to abate PA. Both the modified and the original versions are similar in describing users' behaviour of sidestepping the threat of malicious information technologies such as PA (Arachchilage & Hameed, 2017; Liang & Xue, 2009). The models also explained about the way individual users avoid malicious cyberthreats via making use of a given safeguarding measure. These safeguarding measures do not basically have to be an IT basis like anti-phishing tools; relatively it could be behaviour such as ant-phishing education (Liang & Xue, 2010).

This study employs the modified TTAT to propose and validate the phishing avoidance behaviour of IB users by focusing on the antecedents of perceived threat (perceived severity and perceived vulnerability) and the antecedents of self-efficacy (procedural knowledge and conceptual knowledge) on both perceived threat and self-efficacy and their influence on avoidance motivation and phishing avoidance behaviour (Arachchilage, et al., 2017). Finally, this study also incorporates the moderating role of system trust on the relationship between avoidance motivation and phishing avoidance behaviour of IB users.

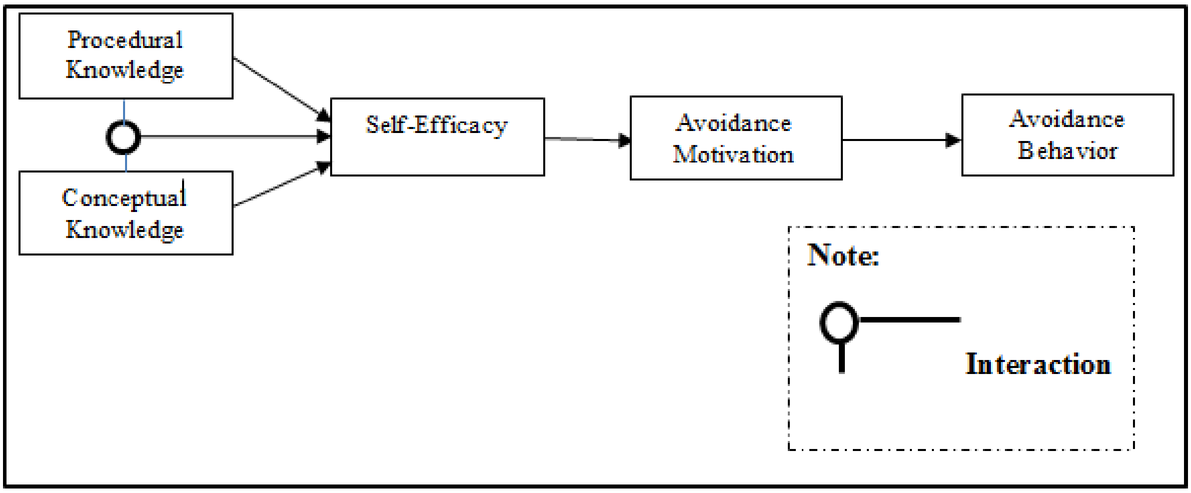


Figure 3: Modified TTAT (Arachchilage & Love, 2014)

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 will also incorporate the system trust as the moderator since it has identified as a major variable 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).

3. CONCEPTUAL MODEL AND HYPOTHESES

3.1. Research Conceptual Model

The conceptual model for the proposed study as shown below in Figure 4 is based on the TTAT and Modified TTAT (Arachchilage & Love, 2014; Liang & Xue, 2009). Comprises of nine interdependent determinants of success, this model suggests that perceived severity will significantly have influence on perceived threat. While, perceived vulnerability will significantly have influence on perceived threat. Similarly, interaction between perceived severity and perceived vulnerability will significantly have influence on perceived threat. Likewise, procedural knowledge will significantly have influence on self-efficacy, conceptual knowledge will also have significantly influence on self-efficacy. Furthermore, interaction between procedural knowledge and conceptual knowledge will significantly have influence on self-efficacy. At the second level, perceived threat will significantly influence avoidance motivation., and self-efficacy threat will significantly influence avoidance motivation. As a result of these avoidance motivation will significantly have influence on avoidance behaviour. At the same time, system trust is also expected to moderate the relationship between avoidance motivation and avoidance behaviour among IB users.

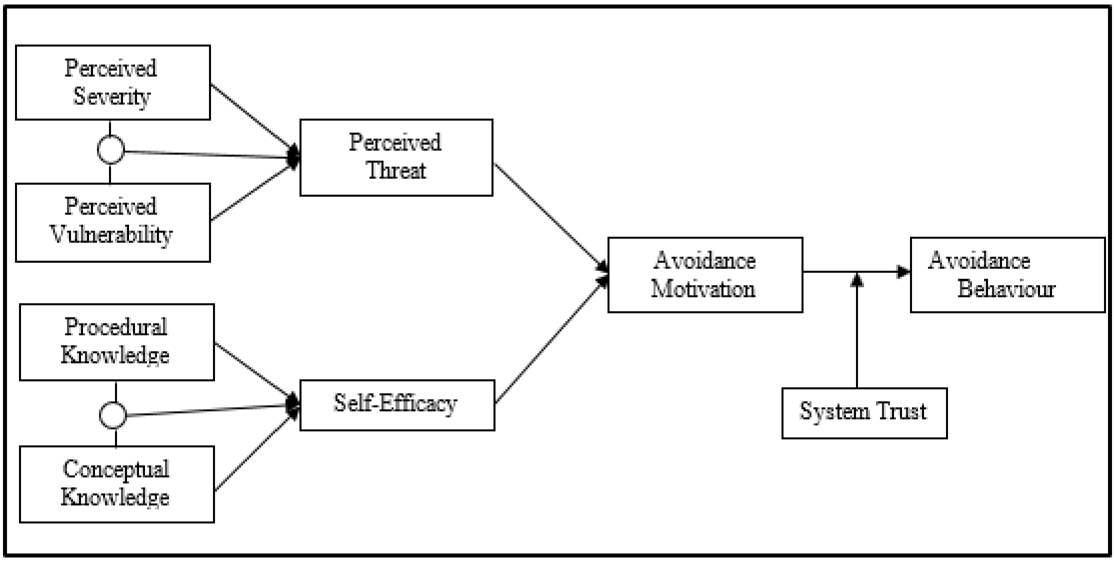


Figure 4: Research Conceptual Model

3.2. Hypotheses

The current study postulated that Perceived Severity would positively influence Perceived Threat among IB user's in Nigeria, in a positive relationship. PSE refers to the alleged harmful consequences of the circumstances (Nguyen, 2013). This assumption was supported by many previous studies that proved the significant relationships between PSE and PTH (Carpenter, et al., 2019; Boysen, Hewitt, Gibbs & McLeod 2019; Boysen, 2018). Likewise, the study of Liang and Xue (2009, 2010) developed and tested a technology threat avoidance model to find that the motivation to avoid spyware was affected positively by the perceived threat (susceptibility and severity). Hence, the upcoming main hypothesis is suggested for this study.

H_1: Perceived Severity have the significant influences on Perceived Threat among IB users

Many published works have described the correlation between PVU and PTH. PVU is regarded as the perceived likelihood of contracting an illness/ attacks (Nguyen, 2013). This assumption was supported by many previous studies that proved the significant relationships between PVU and PTH (Carpenter, et al., 2019; Boysen, et al., 2019; Boysen, 2018). Findings from Liang and Xue, (2010) stressed that perceived threat is determined by perceived susceptibility and severity and fully mediates their effects. Besides, PVU and PTH did not moderate the relationship between the other predictor variables and medicating intention (Wise, 2017). However, Researchers have created exact questions to measure personal vulnerability in every case. Even though there have been some efforts to measure PVU, until now, the literature has failed to include a full scale to measure this, because the concept of PVU signifies a subjective perceived risk with diverse reasoning understandings for everyone (Wise, 2017; Durvasula, Andrews & Netemeyer, 1997). Hence, the following main hypothesis is proposed, and the detailed discussions of the sub-hypotheses are provided in the next paragraphs.

H2: Perceived Vulnerability have the significant influences on Perceived Threat among IB users

Providing users with more information about the threat of online fraud could increase their perceptions of vulnerability. It is also noted that the threat itself is not necessarily the direct link to behaviour change but that the fear produced from such threats is something that people wish to resolve, and hence indirectly threat should affect behaviour (Janis, 1974). Liang and Xue (2010) contend that PVU and PSE have an interaction effect when shaping the threat perception. The interaction between PVU and PSE perceptions suggests that the relationship between either of them and PTH will disappear if the other variable is scored zero. Similarly, when individuals perceive that a malicious IT has no chance of bothering them, they are unlikely to feel threatened, even if the malicious IT can cause serious damages. They will also not feel threatened when they believe that the harmful outcome of a malicious IT is not at all severe, no matter how likely it is to occur. The interaction between PVU and PSE is basically a moderation phenomenon. That is, PVU positively moderates the relationship between PSE and threat, or vice versa. This study proposes the following hypothesis based on the earlier discussion:

H_3: The interaction between Perceived Severity and Perceived Vulnerability have the significant influences on Perceived Threat among IB users

According to McCormick (1997) who has stated that knowledge can be influenced by learning procedural knowledge associated with technological activities. According to Plant, (1994) that argued that PK is close to the ideal of "know how", in which the ideas are imperative to educate one to thwart phishing attacks (Arachchilage, et al., 2017; Arachchilage, et al., 2014). This suggests that there are some boundary conditions that could explain why some people might not act on their self-efficacy beliefs. The study of Baral and Arachchilage, (2019) focuses on investigating the knowledge factors or attributes that enhance the user's self-efficacy in phishing threat avoidance behaviour. The theoretical model investigated the effect of PK on user's self-efficacy to combat against phishing threats. Consequently, the current study puts forward the following hypothesis:

H4: Procedural Knowledge have the significant influences on Self-Efficacy among IB users

Conceptual knowledge is concerned with relationships among ‘items’ of knowledge. McCormick (1997) has revealed that one’s knowledge can be influenced by learning procedural and conceptual knowledge associated with the study of (Plant, 1994) that argued that CK is close to the idea of “know in which the ideas are imperative to educate one to thwart phishing attacks (Arachchilage, et al., 2017; Arachchilage, et al., 2014). Furthermore, his research work described that CK certify one to explain why, hence the difference of know-how and know why (Arachchilage, et al., 2017). Additionally, McCormick (1997) stated that the two ideas of CK and PK are regularly treated individually, with their relationship being ignored. From previous study of Baral, et al. (2019) have been able to include observational knowledge, heuristic knowledge and structural knowledge in the TTAT based theoretical model of (Liang, et al., 2010). The preceding discussion is therefore the basis for the current study’s proposal of the hypothesis:

H_5: Conceptual Knowledge have the significant influences on Self-Efficacy among IB users

The theoretical model of Arachchilage et al. (2014) examined whether CK and PK have effects on computer users’ SEF to thwart phishing attacks. Their findings revealed that the interaction effect of both PK and CK, will positively influence on SEF, which contributes to enhance computer users’ PA avoidance behaviour via the help of their motivation (Arachchilage et al., 2014). Moreover, one can argue that presenting the player with diverse kinds of URLs to detect if it is phishing (fake) or legitimate (PK) then asking them to identify which part of the URL is phishing (CK), would positively impact on his/her SEF to boost the phishing threat avoidance. The current research work integrates either PK or CK (the interaction effect of both PK and CK) into an anti-phishing educational game to better edify people how to guard themselves against PA (Arachchilage, et al., 2017). Thus, conceptual CK and PK identifies that there is a positive effect on computer users’ SEF in relation to thwarting PA. The following hypothesis is thus put forward:

H_6: The interaction between Procedural Knowledge and Conceptual Knowledge have significant influences on Self-Efficacy among IB users

IT threats can cause painful privacy and financial losses. Thus, when users perceive an IT threat, they are motivated to avoid it (Arachchilage, et al.., 2013). Avoidance motivation is defined as the degree to which IT users are motivated to avoid IT threats by taking safeguarding measures (Carpental, et al., 2019). As the threat perception intensifies, individuals are more motivated to get away from the danger (Boysen, et al., 2019; Boss, et al., 2015). As Liang and Xue (2009) articulate, malicious IT and diseases are similar because both are rogue agents that invade a system to cause malevolent changes. Therefore, people’s responses to health threats tend to be similar to their responses to IT threats. Consequently, the more the users feel that they are at risk or that the chances of being affected by a given IT threat are high, the more likely they will be motivated to engage in protective actions (Alsaleh, Alomar & Alarifi, 2017). Based on the empirical evidence from health psychology, we propose that perceived threat of malicious IT positively affects avoidance motivation (Arachchilage, et al., 2016). Therefore, based on this argument, the current study puts forward the following hypothesis:

H_7: Perceived Threat have significant influences on Avoidance Motivation among IB users

Self-efficacy has a co-relation with individuals’ knowledge (Hu, 2010). While self-efficacy is known to play a vital role in influencing security behaviours, the relationship is sometimes weak or even non-significant (Martens, De Wolf & De Marez, 2019; Menard, Warkentin & Lowry, 2018). Pursuing further, current literature from earlier research has also revealed that there is a strong relationship between people’s SEF and their active involvement and achievements (Baslyman & Chiasson, 2016). Bandura in (1977) defined self-efficacy as one’s own judgments about their competences to create and implement activities to obtain positive target. According to authors in (Arachchilage, et al., 2017), it is necessary to build threat perception in user so that they will motivate themselves to combat phishing attack through their avoidance behaviour. On the other hand, SEF leads to individual's better threat perception and such threats are available on the cyber space. Hence, the current study proposed the following hypothesis:

H$_8$: Self-Efficacy have significant influences on Avoidance Motivation among IB users

So far, there has been little work on end-user behaviour on performing security and averting users from attacks such as PA (Arachchilage, et al., 2017; Arachchilage, et al., 2016; Arachchilage, et al., 2013). 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. Arachchilage and Love (2016) proposed and established a game framework which improved user avoidance behaviour through motivation by protecting users from phishing attacks. Besides, a theoretical model derived from TTAT was used in the game design framework. The TTAT acknowledged the issues that the game design framework desirable to discourse by emerging threat insights that inspired individuals to evade phishing attacks and use safeguarding measures (Orunsolu, et al., 2017). Pursuing further, Liang and Xue, (2010); Young, (2016) emphasised that subsequent test of the theory in the context of anti-spyware software usage offered backing for most of the theory's key proposals. User's avoidance motivation is frequently strongminded thru three ideas such as safeguard effectiveness, safeguard cost, and self-efficacy (Arachchilage & Cole, 2011).

H$_9$: Avoidance Motivation have significant influences on Avoidance Behaviour among IB users

Though there is a lack of study on System Trust (ST) that focusing on Avoidance Motivation (AM) and Phishing Avoidance Behaviour (PAB). A challenging problem, however, has been the difficulty that humans have in making effective and accurate trust decisions when dealing with phishing attacks (Misra, et al., 2017; Kumaraguru et al, 2007; Arachchilage, et al., 2014). Trust is significant for bank customers relationships and for customer relationships in over-all, for quite a number of reasons (van Esterik-Plasmeijer, et al., 2017), trust facilitates transactions with customers. To a certain degree, ST is trust in banks at large, trust within the banking network is also pertinent here (Bülbül, 2013). ST is also denoted to as wide scope trust which is regarded as hope apprehended unto by customers that companies within a certain businesses type are commonly relied on to deliver their promises (van Esterik-Plasmeijer, et al., 2017; Sirdeshmukh, Singh & Sabol, 2002). Besides, high level of trust is a buffer against negative experiences which can arise amongst customers. With a low level of trust, however, a negative experience may be perceived as a "proof" that the bank cannot be trusted in any way. The banking system and specific banks are alleged being part/origin of the economic tragedy. Therefore, trust has been broken and must be well-thought-out from both wide scope as well as narrow scope perspective (van Esterik-Plasmeijer, et al., 2017; Gillespie & Hurley, 2013; Grayson, Johnson & Chen 2008). Therefore, based on this argument, the current study puts forward the following hypothesis:

H$_{10}$: System Trust moderates the relationship between Avoidance Motivation and Phishing Avoidance Behaviour among IB users.

4. METHODOLOGY

A cross-sectional survey field study will be employed in this study, as the data will be collected at a single point in time. The choice of the cross-sectional design was in-line with Babbie (2010); Sekaran and Bougie (2010) which established the use of cross-sectional studies as having advantages over the longitudinal study because the researcher, aimed at collecting data that reflects peoples' opinion. Applying a survey method is believed to be the most appropriate to choose because it is an accurate means to gather information as well as enable the researchers to generalize the findings, from the sample to a population (Creswell, 2014). This method is also suitable for a research with the large sample size, as the survey is quick, cheap and efficient to administer (Sekaran, 2003). Finally, a survey is appropriate when asking the respondents about their thought, opinions, and feelings (Shaughnessy, Zechmeister, & Zechmeister, 2012).

4.1. Sampling

This study will use the probability sampling method to reduce the bias and increase the generalizability of the findings. The data of the study will be collected randomly via structured questionnaires from 280 users of IB in Nigeria. The respondents were drawn from four stratified selected commercial banks that have branches in Lagos State, Nigeria. These banks were chosen because of their considerable leading roles and investment in online banking facilities, as they are equally ranked as the most customers focused banks (KPMG, 2013, 2014). Selections of these banks will also increase external validity of the results (AbuShanab, Pearson & Setterstrom, 2010). Based on confidentiality, the questionnaires will be distributed systematically to the customers through their addresses by the head of operations of each bank as it is the policy of the banks not to avail researchers with the contacts of their customers. This method of distribution was used as experience has shown that IB customers do not often come to the branches for transactions and to equally avoid any bias that may be associated with convenient method of distribution being used by previous studies (Mann and Sahni, 2013; Safeena, Date, and Kammani, 2011). The method of distributing questionnaires through the banks was also used by (Salimon, Yusoff & Mohd Mokhtar, 2017; Al-Smadi 2012). It should be noted however that the process of distribution and collection spanned close to four months as the researchers followed up throughout the period to ensure a fruitful exercise.

4.2. Instrument Design

This study has systematically developed the questionnaire that meets the research objectives based on the proposed Conceptual Model. The questionnaire is divided into ten parts. Part A addressed the demographic profile of the respondents. Part B focuses on the measurement of Phishing Avoidance Behaviour. Followed by Part C which entails measurement of Avoidance Motivation. Part D presents measurement of System Trust. Part E which entails measurement of Self-Efficacy. Part F which entails the measurement of Perceived Threat. Part G entails Conceptual Knowledge. Part H presents measurement of Procedural Knowledge. Part I depicts Perceived Vulnerability and Part J entails measurement of Perceived Severity. Respondents are asked to tick the appropriate response. In addition, an introductory statement for every construct of the research model has been included in the questionnaire. For the purpose of validation, experts in the study field have revised the formulation of these statements before conducting the pilot study. The content validation was done by seven experts in IS, internet banking experts, IT administrators, and security experts using Content Validity Index (CVI). Furthermore, the face validation was done. As a result, a validated instrument to measure phishing avoidance behaviour among the IB users has been produced, which is ready to be applied in the real study.

The measurement scale for every construct in this study is based on five-point Likert Scale, which ranges from 1 to 5 [‘1’ strongly disagree to ‘5’ strongly agree]. Dwivedi, Khan and Papazafeiropoulou (2007) stressed that five-point likert scale is the most acceptable likert points due to the convenience it creates for the respondent in making choice. This is buttressed by Muraina, (2015), Woodcock, Middleton and Nortcliffe, (2012) that respondents of questionnaires on the usage of technology face no difficulty while administering questionnaires designed in five-point likert scale. Therefore, Table 1 present the validated measurement for each variable.

Table 1: Measurement of Variables

Variable/Items

Phishing Avoidance Behaviour:

1. I know how to avoid phishing attacks on internet banking platforms
2. I update my anti-phishing knowledge frequently
3. Updating anti-phishing knowledge is not very important to avoid phishing attacks

Avoidance Motivation:

1. I intend to obtain anti-phishing knowledge to avoid phishing attack
2. I predict that I would gain anti-phishing knowledge to avoid phishing attack
3. I feel that I do not want to gain anti-phishing knowledge to avoid phishing attack

System Trust:

1. I believe my internet banking service provider adheres to a set of rules which protects my bank details
2. I believe my internet banking service provider is competent and trustworthy
3. I believe my personal and banking information are well protected by my internet service provider
4. I believe my privacy is assured with my internet service provider
5. I trust my internet banking system’s security features

Self-Efficacy:

1. I could successfully gain anti-phishing knowledge if I had never learned it before
2. I could successfully gain anti-phishing knowledge if I had only related resources for reference
3. I could successfully gain anti-phishing knowledge if no one else helped me get started
4. I could successfully gain anti-phishing knowledge if I had a lot of time
5. I could successfully gain anti-phishing knowledge if no one taught me how to do it first

Perceived Threat:

1. Using internet bank on public/unsecured computers possess a threat to my account
2. The trouble caused by public/ unsecured computers threatens me
3. Using internet bank on public/ unsecured computers exposes my banking details
4. I am dreadful to sign-in on my internet bank account on a computer infected by spyware
5. It is risky to sign-in on my internet bank account on any computer with spyware

Conceptual Knowledge:

1. https://ibank.accessbankplc.com/ internet-banking/RetailBank/#/
2. https://www.gtbank.com/internet-banking
3. https://www.zenithbank.com/internet-banking/personal-banking/
4. https://ibank.accessbankplc.com/RetailBank/#/
5. https://www.gtbank.com/personal-banking/ways-to-bank/internet-banking
6. https://www.zenithbank.com/internet-banking/

Procedural Knowledge:

1. I know how to implement anti-phishing techniques on Internet bank system
2. I know how to prevent my details from attackers from my Internet banking system
3. I know how to make my password hard for hackers
4. I do not reveal my banking details to anyone
5. Sometimes, I share my Internet bank log-in details with my close friends/family

Perceived Vulnerability:

1. I could be subject to a serious information security threat
2. I am facing more and more information security threats
3. I feel that my device could be vulnerable to a security threat
4. It is likely that my device will be compromised in the future
5. My information and data are vulnerable to security breaches
6. I could fall victim to a malicious attack if I fail to follow good security

Perceived Severity:

1. A security breach on my computer would be a serious problem for me
2. Loss of information resulting from hacking would be a serious problem for me
3. Having my confidential information on my device accessed by someone without my consent or knowledge would be a serious problem for me
4. Having someone successfully attack and damage my device would be very problematic for me
5. I view information security attacks on me as harmful
6. I believe that protecting the information on my device is important

4.3. Data Analysis Procedure

The data analysis process will be conducted in two phases. In the first phase, SPSS Statistics (SPSS) will be used for data entry, screening, and preparation, for the purpose of identifying missing and non-compliance data before starting the main analysis. Finally, in the second phase, Structural Equation Modelling (SEM) will be used for hypotheses and model testing. In addition, PLS-SEM allows the modelling among multiple exogenous latent variables and latent endogenous variables simultaneously (Gefen, Straub, & Boudreau, 2000). According to Hair, Ringle, and Sarstedt (2011), SEM is an appropriate multivariate method to test the complete theories and concepts. Moreover, it enables the researcher to conduct systematic and comprehensive testing of the interlinked variables and their items in just a single run (Gefen, et al., 2000)

5. CONCLUSION

This paper has presented the initial stage of the study which comprises of introduction, objectives, literature review, conceptual framework and research methodology that will be employed. From the literature analysis, the research issues and the gaps have been identified. Building on this, a research conceptual framework is developed to evaluate the phishing avoidance behaviour among IB users in Nigeria. Furthermore, this study will be beneficial to the researchers in both domains on, IS, banks and services providers by contributing in the following ways. First, this study will examine the applicability of TTAT Model to evaluate the phishing avoidance behaviour. Second, this study will extend the TTAT Model, by testing the role of System Trust as the moderating variable between two relationships namely, Avoidance Motivation and Avoidance Behaviour. By examining these moderating effects, the study aims to improve the explanation power of TTAT in the context of IB application. Nevertheless, no study is yet to examine the moderating role of System Trust on TTAT Model nor on the Modified TTAT. Finally, this study posits that all constructs are significant, especially in capturing issues on threats.

In conclusion, this 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 application of phishing avoidance behaviour relies upon its ability to meet the users’ requirement and expectation, regardless of the location. 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, for future improvement, as well as to justify their asset.

REFERENCES

[1] 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.

[2] Sánchez-Torres, J. A., Canada, F. J. A., Sandoval, A. V., & Alzate, J. A. S. (2018). E-banking in Colombia: factors favouring its acceptance, online trust and government support. International Journal of Bank Marketing, 36(1), 170-183.

[3] 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.

[4] Fadare, O. A. (2015). A survey on perceived risk and intention of adopting internet banking. The Journal of Internet Banking and Commerce, 21(1).

[5] 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.

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

[7] 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.

[8] Hameed, M. A., & Arachchilage, N. A. G. (2016). A Model for the Adoption Process of Information

[9] System Security Innovations in Organisations: A Theoretical Perspective. In: The Proceeding of the 27th Australasian Conference on Information Systems, arxiv.org/abs/1609.07911.

[10] 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).

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

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

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

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

[15] 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.

[16] Tambe Ebot, A. C. (2017). Explaining Two Forms of Internet Crime from Two Perspectives: Toward Stage Theories for Phishing and Internet Scamming. Jyväskylä Studies in Computing, (259).Hatunic-Webster, A. (2017). Anti-Phishing Models: Main Challenges.

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

[18] Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In 2016 international conference on computing, communication and automation (ICCCA) (pp. 537-540). IEEE.

[19] Ghosh, D., Li, C., & Yang, C. (2018). A Lightweight Authentication Protocol in Smart Grid. IJ Network Security, 20(3), 414-422.

[20] Chaudhary, S. (2016). The Use of Usable Security and Security Education to Fight Phishing Attacks. Arachchilage, N. A. G., & Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. Computers in Human Behaviour, 38, 304-312.

[21] 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).

[22] ACM. 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.

[23] 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.

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

[25] 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).

[26] Rader, E., & Wash, R. (2015). Identifying Patterns in Informal Sources of Security Information. Journal of Cyber security, 1(1), 121-144.

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

[28] Tsai, W. H., Huang, B. Y., Liu, J. Y., Tsaur, T. S., & Lin, S. J. (2010). The application of Web ATMs in e-payment industry: A case study. Expert Systems with Applications, 37(1), 587-597.

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

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

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

[32] 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.

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

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

[35] 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.

[36] Arachchilage, N. A. G., & Hameed, M. A. (2017). Integrating Self-Efficacy into a Gamified Approach to Thwart Phishing attacks. arXiv preprint arXiv:1706.07748.

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

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

[39] Nguyen, P. (2013). Mothers’ Perceived Vulnerability, Perceived Threat and Intention to Administer Preventive Medication to Their Children. Contemporary Management Research, 9(4), 399-418.

[40] Boysen, S., Hewitt, B., Gibbs, D., & McLeod, A. (2019). Refining the Threat Calculus of Technology Threat Avoidance Theory. Communications of the Association for Information Systems, 45(1), 5.

[41] Boysen, S. D. (2018). Analysing Threat Perceptions in the Context of Fitness Data: Refining the Technology Threat Avoidance Theory.

[42] Wise, J. A. (2017). Perceived Vulnerability in Consumer Ethnocentrism. International Journal of Business and Social Research, 7(11), 21-30.

[43] Durvasula, S., Andrews, J. C., & Netemeyer, R. G., (1997). A Cross-Cultural Comparison of Consumer Ethnocentrism in the United States and Russia. Journal of International Consumer Marketing, 9, 73-93.

[44] Janis, I. (1974). Vigilance and Decision making in Personal Crises. In G. Coelho, D.Hamburg, & R. J. Adams (Eds.), Coping and adaptation. New York: Basic Books.

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

[46] 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.

[47] 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 Cyber security and Cyber forensics Conference (CCC) (pp. 102-110). IEEE.

[48] Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone Users: Understanding how Security Mechanisms are Perceived and New Persuasive Methods. PloS One, 12(3), e0173284.

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

[50] Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and Comparing the Predictors of the Intention towards taking Security Measures against Malware, Scams and Cybercrime in General. Computers in Human Behaviour, 92, 139-150.

[51] 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

[52] Baslyman, M., Chiasson, S (2016). Smells Phishy?: An Educational Game about Online Phishing Scams. In: APWG Symposium on Electronic Crime Research (eCrime). pp. 1–11. IEEE.

[53] Bandura, A. (1977). Self-Efficacy: Toward a Unifying Theory of Behavioural Change. Psychological Review, 84(2), 191.

[54] Orunsolu, A. A., Sodiya, A. S., Akinwale, A. T., Olajuwon, B. I., Alaran, M. A., Bamgboye, O. O., & Afolabi, O. A. (2017). An Empirical Evaluation of Security Tips in Phishing Prevention: A Case Study of Nigerian Banks. International Journal of Electronics and Information Engineering, 6(1), 25-39.

[55] Arachchilage, N. A. G., & Cole, M. (2011). Design a Mobile Game for Home Computer Users to Prevent from “Phishing Attacks”. In Information Society (i-Society), 2011 International Conference on (pp. 485-489). IEEE.

[56] Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., et al. (2007). Getting users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. In APWG ecrime Researchers Summit, Pittsburgh, PA, USA,October 4–5, 2007

[57] Bülbül, D. (2013). “Determinants of Trust in Banking Networks”, Journal of Economic Behaviour &Organization, Vol. 85, Special Issue, pp. 236-248.

[58] Sirdeshmukh, D., Singh, J., & Sabol, B. (2002). Consumer Trust, Value, and Loyalty in Relational Exchanges. Journal of Marketing, 66(1), 15-37.

[59] Gillespie, N. and Hurley, R. (2013). “Trust and the Global Financial Crisis”, in Bachmann, R. and Zaheer, A. (Eds), Handbook of Advances in Trust Research, Edward Elgar, Cheltenham, pp. 177-203.

[60] Grayson, K., Johnson, D. & Chen, D.-F.R. (2008). “Is Firm Trust Essential in a Trusted Environment? How Trust in the Business Context Influences Customers”. Journal of Marketing Research, Vol. 45 No. 2, pp. 241-256.

[61] Babbie, E. (2010). Research Design. The Practice of Social Research, 85-88.

[62] Sekaran, U., & Bougie, R. (2010). Research Design. JW Ltd, Research Methods for Business-, 110.Creswell, J. W. (2014). Research Design: Qualitative, Quantitative and Mix Methods Approaches (4th Sekaran, U. (2003). Research Methods for Business: A Skill Building Approach. 4th Ed., New York, USA, John Wiley & Sons, Inc.

[63] Shaughnessy, J. J., Zechmeister, E. B., & Zechmeister, J. S. (2012). Research Methods in Psychology (9th ed.). New York: McGraw-Hill

[64] KPMG (2013), “Banking industry customer satisfaction survey”, KPMG Professional Services, Lagos, available at: www.Kpmg.com.

[65] KPMG (2014), “Banking industry customer satisfaction survey”, KPMG Professional Services, Lagos, available at: www.Kpmg.com.

[66] AbuShanab, E., Pearson, J.M. and Setterstrom, A.J. (2010), "Internet Banking and Customers' Acceptance in Jordan: The Unified Model's Perspective", Communications of the Association for Information Systems, Vol. 26 No. 1, pp. 494-524.

[67] Mann, B.J.S. and Sahni, S.K. (2013), "Profiling Adopter Categories of Internet Banking in India: An Empirical Study", Vision: The Journal of Business Perspective, Vol. 16 No. 4, pp. 283-295.

[68] Safeena, R., Date, H. and Kammani, A. (2011), "Internet Banking Adoption in an Emerging Economy: Indian Consumer's Perspective", International Arab Journal of E-Technology, Vol. 2 No. 1, pp. 56-64

[69] Salimon, M. G., Yusoff, R. Z. B., & Mohd Mokhtar, S. S. (2017). The Mediating Role of Hedonic Motivation on the Relationship between Adoption of e-banking and its Determinants. International Journal of Bank Marketing, 35(4), 558-582.

[70] Al-Smadi, M.O. (2012), "Factors Affecting Adoption of Electronic Banking: An Analysis of the Perspectives of Banks' Customers", International Journal of Business and Social Science, Vol. 3 No. 17, pp. 294-309.

[71] Dwivedi, Y. K., Khan, N., & Papazafeiropoulou, A. (2007). Consumer Adoption and Usage of Broadband in Bangladesh. International Journal of Electronic Government, Vol. 4, No 3, pp. 299-313.

[72] Muraina, I. D. (2015). The Factors that Contribute to the Continuous Usage of Broadband Technologies Among Youth in Rural Areas: A Case of Northern Region of Malaysia (Doctoral Dissertation, Thesis, Universiti Utara Malaysia).

[73] Woodcock, B., Middleton, A., & Nortcliffe, A. (2012). Considering the Smartphone Learner: An Investigation into Student Interest in the Use of Personal Technology to Enhance their Learning. Student Engagement and Experience Journal, Vol.1, No. 1, pp. 1-15

[74] Gefen, D., Straub, D. & Boudreau, M. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. Communications of the Association for Information Systems. 4 (Article 7), 1-79.

[75] Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed, a Silver Bullet. Journal of Marketing Theory and Practice, 19(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202.

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 behavioral and users' aspects of systems security including acceptance/rejection of security technologies, cyber-crime, motivations for engaging in risky online behavior, and online deception. She is also interested in information privacy, technology adoption/continuance behaviors, and inter-organizational benefits/effects of information systems. She has published in the Journal of Internet Banking and Commerce, Journal of Information System and Technology Management, International Journal of Civil Engineering and Technology and International Journal of Trade, Economics and 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.