Understanding Responses to Phishing in Saudi Arabia via the Theory of Planned Behaviour

Ahmed Alyahya
Department of Computer & Information Sciences
University of Strathclyde
Glasgow, UK
ahmed.alyahya@strath.ac.uk

George R S Weir
Department of Computer & Information Sciences
University of Strathclyde
Glasgow, UK
george.weir@strath.ac.uk

2021 National Computing Colleges Conference (NCCC) | 978-1-7281-6719-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/NCCC49330.2021.9428823

***Abstract*—Saudi Arabia has seen an enormous growth in Internet usage over the past few years. With increasing adoption of this technology has come a rise in cybercrime, often enabled through use of social engineering. Phishing is a prime example, aiming to deceive users into revealing personal data. The paper describes efforts to understand individuals' responses to phishing attacks through application of the Theory of Planned Behaviour (TPB). It reports a survey that considers three common social engineering persuading strategies, Authority, Social Proof and Scarcity. Results show correlations between these strategies and TPB. In particular, between attitude and intention to respond under the Authority strategy; subjective norms and intention to respond under the Social Proof strategy; and subjective norms and intention to respond under the Scarcity strategy.**

Keywords— Social Engineering Persuading Strategies, Phishing, Theory of Planned Behaviour.

I. INTRODUCTION

The total population in Saudi Arabia is about 34.54 million, out of which 32.23 million are Internet users [1]. Aside from its beneficial applications, the Internet affords a great opportunity for miscreants to execute cybercrimes. One widely recognized cybercrime and basis for Internet fraud is phishing [2]. This is 'a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party' [3 p.1]. Elnaim and Al-Lami's study aims to examine knowledge of phishing attacks in university students [2], with a survey of 50 undergraduate students to determine ability to recognize phishing attacks and how to defend themselves. The result showed that, although a majority were Computer Science Students, only 50% were familiar with the term 'phishing'.

Obviously, user behaviour is a major cause of cybercrimes [4] and many such crimes could be prevented if users acted differently. So, in seeking to protect individuals from phishing attacks, it is important to understand behavioural factors that motivate the user's intention when confronted with an exploit. To this end, the present paper considers the Theory of Planned Behaviour [5] to determine whether it could serve to explain user responses to phishing emails in Saudi Arabia.

II. PHISHING

Phishing is a form of social engineering, which is defined by the Anti-Phishing Work Group [6] as a targeted email attack where the attacker convinces the victim to perform actions, such as opening a malicious attachment, visiting a fake web page or clicking on a bad link. Commonly, phishing involves sending emails that appear to be from reliable sources and aim to obtain victim's confidential information, such as bank account details, passwords, etc. There are various types of phishing such as, spear phishing, vishing, SMishing, pharming, Wailing and clone phishing [7] [8]. Over time, the phishers are improving their techniques by developing sophisticated attacks and changing their strategies [9].

Phishing is one of the top ten cyber security challenges [10] and remains the most popular method of security attack [11]. In the third quarter of 2018, according to the Phishing Activity Trends Report published by the APWG, the number of detected phishing websites was 151,014, whereas the number of reported phishing e-mails by APWG consumers was 270,557, and the number of brands targeted by the phishers was 777 [34]. In the second quarter of 2020, it is reported by Kaspersky that Kingdom of Saudi Arabia experienced almost a million phishing attacks, the cybersecurity company says in a new report. A total of 973,061 phishing attacks in the Kingdom were detected in the three months per Kaspersky's spam and phishing report [33].

According to Imperva [12], phishing happens when a hacker impersonates a trusted entity and deceives the target into opening an email. The victim clicks on a link, which can lead to harmful actions such as the installation of malicious software, or the eliciting of personal information.

Benenson [13] explains the reasons behind the clicking behaviour of individuals. Their results revealed that the reasons for clicking were a combination of curiosity, context, known sender, fear and natural behaviour. Underlying phishing as an exploit, which relies upon social engineering, i.e., a way of deceiving people using a range of psychological techniques. According to Arab News [14], more than 90% of malicious software is spread via email and Saudi users have been confronted with more than 30 million phishing emails in the recent years.

III. SOCIAL ENGINEERING STRATEGIES

Social engineering is 'the manipulation of a person or persons to reach an objective by abusing the victim's emotions, gullibility, charity, or trust' [7 p.13]. The persuader attends to human factors such as emotions, fear, desire and greed as a basis for social engineering strategies, in order to manipulate the victim and gather information such as credit card details, passwords and so on. Social engineering attacks can be variously classified. Based on the entity involved, such exploits can be differentiated into two types, direct and indirect [15].

A. Direct

This type of attack involves physical interaction like a conversation or eye to eye contact. Sometimes, the attackers

might be working in the same workspace as the victim. This category is further divided into the following sub-categories:

1. Human-based Attacks – Here, the attackers directly interact with the desired victim and collects as much information as possible. Since it requires human interaction, limited number of individuals can be manipulated. This includes the following sub-categories.
    a. Social-based Attacks - This is the most dangerous as it requires human interactions where, the attacker exploit the psychological and emotional health of the victim [16]. These types of attacks include baiting and spear phishing
    b. Physical-based Attacks - This involves physical activities to gather information regarding the victim. For instance, the attacker might search for valuable information in the dumpsters [17].
2. Indirect – Here, the attacker executes the plan by sending an email containing a hyperlink or downloadable attachment or SMS message. This includes
    a. Software-based attacks – Here, the attacker uses physical device like a computer or mobile phone to collect victim's information. As it does not involve human interaction, innumerable attacks can be launched in seconds [18]. This category includes
    b. Technical-based attacks - This type of attack involves the usage of Internet, social media and websites offering online services. Here, the attacker gathers confidential information including, but not limited to, passwords, bank account information and other security details [19].

Social engineering attacks may use a combination of these categories.

There are numerous theories on social engineering persuasion strategies [20, 21, 22], however, Clandini's psychological persuasion strategies [20] have wide appeal. Clandini recognises six strategies, namely, reciprocation, consistency, liking, authority, social proof and scarcity. Our research focuses on the latter three strategies as they require human interaction, while the former three focuses on recurring relationships and fall outside the scope of this research.

B. Authority

People have a tendency to respect and obey the commands they receive from higher authorities [20, 23, 24], including parents, teachers and work superiors.

C. Social Proof

When people face a situation where they are not able to make decisions, they seek guidance from decisions made by others. This is fine, as long as they are modelling behaviour on people they trust, like family members and close friends. However, if they blindly follow societal trends, then they might face long term consequences. In the worst case, this leads to a phenomenon called pluralistic ignorance. [20]

D. Scarcity

The lack of resources and high demand for a product increases its perceived value and makes it more desirable. Available time is recognised as a stressful factor, it is efficient to make the market see that time is in limited supply, thus leaving no time for reaction [20]. An email might present an item to be available for a limited time and offer a timely discount making it in-demand and valuable.

E. Phishing in Saudi Arabia

According to the Ministry of Communications and Information Technology (MCIT) the number of phishing emails in Saudi Arabia have exceeded 26 million [25].

An experiment was conducted with students at a university in Saudi Arabia, by creating a replica of their official website. Around 200 students volunteered to participate, and they were briefed by saying that the experiment is to learn user behaviour when dealing with phishing attacks. The experiment also involved a trusted instructor, because out of respect, students trust their teachers and complete all the assigned tasks. The instructor instructed the students to log in the university's official website. About 90% of the students, entered the information just to obey the trusted instructor's instruction, by the look and feel of website, and did not consider studying the logo and URL properly. The other 5% had a doubt about the authentication of the website. However, out of trust and respect to the instructor, they entered their credentials. The remaining 5% questioned the authenticity and refused to enter the information. [26]

This example clearly presents how user behaviour is influenced by an environment of trust. Commonly, the phisher seeks to gain the trust of their prey [27, 28]. Later, the phisher plays with the emotions of the prey, e.g., warning of account cancellation or risk of getting hacked, and requests that the user provide information [27].

IV. Theory of Planned Behaviour

In this context of phishing exploits, can we find a plausible model that will facilitate understanding the motivation and behaviour of end users?

The Theory of Planned Behaviour (TBP) aims to find the reason behind specific varieties of user behaviour. In principle, the TPB can characterise how people are motivated to action and assist in understanding how people can change certain behaviour. The theory states that behaviour is controlled by the intentions of the individual. Therefore, from the given intention a particular behaviour can be predicted [5]. TPB have been effectively applied on several behaviours, such as to explain consumers' online behaviour [29], smoking behaviour [30], food selection behaviour [31], and alcohol consumption behaviour [32].

The dependent factor – intention, is influenced by three independent factors, namely,

1. Attitude
2. Subjective norms and
3. Perceived Control Behaviour.

Attitude denotes the individual's approach or personal belief towards particular behaviour to determine if the situation is favourable or unfavourable, positive or negative, good or bad. In other words, attitude is the evaluation of ideas, events, objects or people's behaviour, whereby, the intention of an individual is derived from the attitude they have towards a considered activity or course of action. [5]

Although, attitude cannot easily be measured or captured, one such example is the personal beliefs formed by an individual around the type of content they expect a given email to contain. When an individual receives an email from education institute – such as a University or School – they will have pre-formed notions of the type of content and layout that will be included in the email. For example, does it contain the University Logo, header, signature of the sender, language consistency and quality of content? These factors are taken into consideration by the individuals when encountering a potential social engineering attack, whether to proceed with the email and perform the requested action. However, when it comes to fake government emails, the user is not aware of the country's protocol and with compelling words like urgent, important, the person might fall a victim. For example, during the Covid-19 era, there were many fake emails regarding Covid vaccination in Saudi Arabia and many citizens fell prey to the scam [14]. The attitude should be precisely identified, as it is paramount to enable the successful realization of the perceived resulting behaviour.

Subjective norms or societal expectations/pressure might play a significant role in shaping individual's intention [5]. In other words, the perception formed by an individual relating to their normative beliefs is built through the expectations of that person based on their social circle. In the situation where an individual receives an email from an inconsistent source, the receiver might consider advice from a parent or a friend not to believe the content of such forms of communication.

Perceived behavioural control relates to the ability of an individual to enact a specific behaviour relative to their intention [5]. This can also be framed as the influence or impact of 'control' variables that to a large part sway the decision-making criteria adopted by an individual when deciding to pursue a particular course of action [39].

Using TPB to analyse phishing attacks

To prevent email-based social engineering, various technical precautionary methods have also been proposed, including filtering and content analysis at the server-side, and blacklist-based approaches to prevent users accessing malicious websites [40].

To understand how the users fall a prey to phishing attacks, theory of planned behaviour is used to analyse user responses as intention, according to the theory, is an immediate precursor of actual behaviour [41]. In Information Security studies, the intention is used to predict actual behaviour [36], therefore, it is crucial to examine the role of intention in predicting the actual information security behaviour. The other TPB factors include attitude, Subjective Norms and Perceived Behavioural Control.

Attitude is based on trust as it affects risk-taking in relationships and impacts processes and results in an organization. Trust is defined as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another" [37]. When an employee receives an email, they tend to disregard sender details and focus on the body content, not considering the fact that it might be a phishing email as the set attitude during the business hours are more inclined to official emails rather than phishing emails.

Subjective norms are based on societal pressure where the authenticity of the message is disregarded. An employee might be more inclined to gain approval of colleagues or higher management rather than believing in the genuineness of the emails [42]. Perceived behavioural control is based on pre-notions based on different situations. Marketing companies might send many emails for their product; however, the user can only view the product, and based on their need and financial condition determine whether to purchase the product. Even if the product is purchased, the user might have different views based on the brand or reviews from other users.

A. Relationship between TPB and Phishing emails

According to TPB, attitude, subjective norms and perceived behavioural controls may play a crucial role when individuals consider responding to phishing emails. For instance, when an individual receives a phishing email claiming to come from Netflix regarding the sale on number of users or subscription renewal, the receiver might disregard the verification of email such as seeing the URL and email address. This is because the receiver has a belief (attitude) about the reputed company and does not pay attention to the content of the email. Whereas, the same person, in subjective norm, might consult family and friends regarding the offer and react based on the advice received. In the Perceived behavioural control, based on the person's ability like budget, ease of purchase and decision-making ability, the receiver's intention to the email response is in favour of the phisher.

This study aimed to answer questions such as: (1) Are there correlations between TPB factors and intention towards responding to Authority emails? (2) Are there correlations between TPB factors and intention towards responding to Social Proof emails? (3) Are there correlations between TPB factors and intention towards responding to Scarcity emails?

V. METHODOLOGY

A questionnaire was designed to address subjects' reactions to specific phishing email scenarios. The importance of the behavioural intention in anticipating society and individual behaviour was emphasized by the pioneer of TPB - Ajzen Izek [41], who argued that factors influencing behavioural intention are pre-conceived beliefs of the individual about the possible consequences of their behaviour, beliefs about the normative expectations of others, and beliefs about factors which may ease or prevent the performance of the action [60]. The stronger the intention to perform a behaviour, the more likely the behaviour will be performed [61].

The survey questions used Likert scales, from 1-5 for disagreement and agreement towards given statements. Also, the nine emails were built after studying the genuine phishing examples encountered in Saudi Arabia, based on statistical reports such as Data reportal, a platform that offers free reports on the most widely visited applications and websites [1]. In the associated survey, subjects were asked to consider whether such emails important for them (attitude), recommendations from family and friends to respond to the email (subjective norms), and whether responding to the email is solely the user's decision (Perceived Behavioural Control).

A. Instrument

The survey was conducted in King Faisal University with under-graduate students from Medicine, Computer Science, Engineering and Business Administration. There were 501 recorded responses used to consider correlation between the

independent and dependent variables. The questionnaire followed guidelines by Ajzen Izek and other researchers [60][66][67]. Nine emails were presented, three were focused on each of the Social Engineering strategies - Authority, Social Proof and Scarcity. Each email type had ten questions to test the main independent factors of TPB, namely, attitude (3 questions), subjective norms (2 questions), perceived behaviour control (3 questions); and dependent factor - intention (2 questions). Full details of the questionnaire and scenarios are available on request from the first author.

Cronbach's alpha was used in this study to verify the reliability of the constructs. For basic research reliability, a minimum alpha of 0.7 is recommended [46]. The table 1 demonstrates the Cronbach's alpha projected scale where each variable satisfied the minimum alpha criteria of 0.7. Therefore, the constructs' reliability was considered high and acceptable for this study.

Table I: Reliability Coefficient

Name	Cronbach's Alpha	Number of Items
Attitude	.884	27
Subjective norms	.893	18
PBC	.875	27
Intention	.867	18

VI. Findings

The findings of this study focus on three independent variables: attitude, subjective norms and perceived behavioural control in responding to phishing emails in Saudi Arabia under social engineering persuading strategies.

Table II: Results of phishing emails for all constructs

Social Engineering Persuading Strategies (SEPS)	**Theory of Planned Behaviour (TPB)**			
	Independent Factors			Dependent factors
	Attitude (mean)	Subjective Norms (mean)	PBC (mean)	Intention (mean)
Authority	4.10	3.39	3.77	3.85
Social Proof	2.27	2.29	3.13	2.45
Scarcity	3.17	3.06	3.55	3.22

A. Descriptive Statistics

Table II demonstrates the mean scores for TPB factors under the three social engineering persuading strategies implemented in phishing emails. Scores are based on Likert scale (1-5). Attitude under Authority strategy, Perceived Behaviour Control under Social Proof and Perceived Behaviour Control under Scarcity was identified with the highest mean at 4.10 (between Agree and strongly agree), 3.13 (between neutral and agree) and 3.55 (between neutral and agree) respectively.

B. Correlation Between TPB and Phishing Emails under Social Engineering Persuading Strategies

The correlation coefficient was used to test the relationship between variables [43]. Since the data from this study is not normally distributed, Spearman's rho coefficient correlation is used. The survey sought to gauge the relationship between TPB factors and the intention variable as well as phishing emails. Previous studies that used TPB to determine general user responses reported that attitudes, subjective norms and PBC were linked with user intention [44], [45]. Additionally, Cronbach's alpha evaluated internal consistency for all TPB variable [46]. The findings provided satisfactory levels of reliability with the alpha coefficients of the TPB's elements. So, this study aligns with guidelines on TPB developed by Ajzen [48] and recommended by Francis et. al. [46], which strengthens the findings between attitudes, subjective norms, PBC and user intentions towards responding to phishing emails [5],[46].

The aim of this study was to gauge the application of TPB to phishing email under Social Engineering Persuading Strategies. Table III shows results from the correlation test to determine relationships between the variables. Correlation coefficients range from +1 which reflects a 100% positive relationship, 0.0 represents no relationship and -1.00 reflects a negative relationship [57].

The responses to phishing emails between the correlation factors are as follows: (i) coefficient correlation between the Attitude and the intention to respond to phishing emails under Authority email is at .700 and probability (p) close to 1 (in this study one is the intention); (ii) coefficient correlation between the subjective norms and intention to respond to phishing emails under Social Proof is at .692 and probability close to 1; (iii) coefficient correlation between the subjective norms and intention to respond to phishing emails under Scarcity strategy is at .700, probability close to 1.

Table III: Correlation between TPB factors and phishing emails under social engineering strategies

		ATT	**SN**	**PBC**	**Intention**
Authority	Correlation Coefficient	.700**	.633**	.533**	1
	Sig. (2-tailed)	0.000	0.000	0.000	.
Social Proof	Correlation Coefficient	.638**	.692**	.229**	1
	Sig. (2-tailed)	0.000	0.000	0.000	.
Scarcity	Correlation Coefficient	.658**	.700**	.437**	1
	Sig. (2-tailed)	0.000	0.000	0.000	.

** Correlation is significant at the 0.01 level (2-tailed)

The results of the study strongly support the application of TPB variables in identifying factors that assist in predicting behavioural intentions when encountering phishing emails [5]. Users' behavioural intentions can be predicted by attitudes, subjective norms and PBC [5] as there were significant positive correlations between the belief-based measures of TPB factors and responding to phishing emails under Social Engineering Persuading Strategies.

VII. Discussion

In keeping with other studies [64][65], the correlation between the Attitude and the intention to respond to phishing under the Authority email is higher as the user is likely to trust

and respect authority showing that attitude has a positive and significant relationship with behavioural intention. For instance, when a Saudi citizen receives an email from say, the Ministry of Health, they are less likely to question the content. Thereby establishing a specific attitude when reading and responding to the email.

The correlation between subjective norms and intention to respond to phishing emails under Social Proof strategy occurs as the user is likely to follow the trend in providing feedback or checking out the notification about a particular social media platform. An earlier study proposed the impact of subjective norms on intention toward clicking on phishing e-mails [63]. Similarly, subjective norm is a powerful predictor for intention and the relation was positive and significant with intention [64]. Saudi citizens may be more vulnerable in this setting as the culture is more socializing and people look to make new friends, connections or participate in reviewing or providing their opinion. The last correlation, between subjective norms and intention to respond to phishing emails, under the Scarcity strategy may arise with trending products where the phishers create an email with limited time price offer for the trending product. In line with previous work [63], subjective norms determine responses to phishing email.

Another finding of significance has implications for the sufficiency assumption of the theory of planned behaviour. According to TPB, the information effect on intentions is intervened by attitudes, subjective norms, and perceptions of behavioural control. Studying the TPB model and variables should provide sufficient insight to forecast user intentions and behaviour. However, the data showed a direct effect on intentions, not mediated by attitudes, subjective norms, and perceived behavioural control. A methodological explanation would attribute the different observation in the measurement of the theory's constructs [60].

VIII. Conclusion

A strength of this study is the collection of data for dependent (Intention) and independent variables (Attitude, Subjective Norms and Perceived Behavioural Control). Few studies correlate social engineering persuading strategies with theory of planned behaviour.

Phishing attacks manipulate users to gain access to their confidential information. Users can be educated about phishing, but it is nearly impossible to eliminate the phishing risk. This study is limited in considered culture, reflecting the behaviour of Saudi users. The participants were not trained on phishing attacks, and we might expect some effect on the results following such training. Indeed, the findings reported here should motivate the information security community to improve current training programs and design effective interventions against the perennial risks of phishing-based social engineering attacks. Future work will expand this study to other cultures, organisations and age groups, to consider user behaviour from the perspective of the Theory of Planned Behaviour.

References

[1] Datareportal. 2020. Digital 2020: Saudi Arabia. Available at : https://datareportal.com/reports/digital-2020-saudi-arabia [Accessed : 14/11/2020]

[2] B. Elnaim, and H. AlLami, "The Current State of Phishing Attacks against Saudi Arabia University Students," *Journal of Computer Applications Technology and Research*, vol. 6, no. 1, pp. 42-50, 2017.

[3] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," *Communications of the ACM* , vol. 50, no. 10, pp. 94-100, 2007.

[4] R. Crossler, A. Johnston, P. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioural information security research," *Computers and Security* , vol. 32, no. 5, pp. 91- 101, 2013.

[5] I. Ajzen, "The Theory of Planned Behaviour," *Organizational Behaviour and Human Decision Processes*, vol. 50, no. 4, pp. 179-211, 1991.

[6] APWG. 2014. Phishing Activity Trends Report, 4th Quarter 2014, https://docs.apwg.org/reports/apwg_trends_report_q4_2014.pdf

[7] R. Alabdan, "Phishing Attacks Survey: Types, Vectors, and Technical Approaches," *MDPI Future Internet* , vol. 12, no. 10, pp. 1-39, 2020.

[8] K. Chiew, K. Yong, C. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems With Applications*, vol. 106, pp. 1-20, 2018.

[9] J. Hong, "The state of phishing attacks," *Commun. ACM*, vol 55, no. 1, pp. 74-81, 2012.

[10] Upadhyay, I. 2020. Top 10 Challenges of Cyber Security Faced in 2020. Available at : https://www.jigsawacademy.com/blogs/cyber-security/challenges-of-cyber-security/ [Accessed : 20/01/2021]

[11] R. Griffin, "Evaluating the impact of training and education to counteract social engineering attacks in organisations", Dublin: Dublin Institute of Technology, 2017.

[12] Imperva. 2020. Phishing attacks. Available online : https://www.imperva.com/learn/application-security/phishing-attack-scam/. [Accessed at : 04/05/2020]

[13] Z. Benenson, F. Gassmann, and R. Landwirth, "Unpacking Spear Phishing Susceptibility," *International Conference on Financial Cryptography and Data Security*, DOI https://doi.org/10.1007/978-3-319-7027-0-39, pp. 610-627, 2017.

[14] Arab News. 2020. Cybercriminals target Saudis with vaccine data fraud. Available at : https://www.arabnews.com/node/1787841/saudi-arabia [Accessed : 10/01/2020]

[15] S. Fatima, and K. Naima, K. 2019. "Social Engineering Attacks: A Survey," *MDPI Future Internet*, vol. 11, no. 4, pp. 1-17, 2019.

[16] P. Patil, and P. Devale, "A literature survey of phishing attack technique," *International Journal Advanced Research in Computer and Communication Engineering*, pp. 198–200, 2016.

[17] N. Pokrovskaia, "Social engineering and digital technologies for the security of the social capital' development," *International Conference of Quality Management, Transport and Information Security, Information Technologies, IEEE* , pp. 16–19. 2017.

[18] L. Xiangyu, L. Qiuyang, S. Chandel. 2017. "Social engineering and Insider threats,". *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, IEEE*, pp. 25–34. 2017.

[19] R. Kalnin, J. Purin, G. Alksnis, "Security evaluation of wireless network access points," *Applied Computer Systems*, vol. 21, pp 38–45. 2017

[20] R. Cialdini, "Influence: The Psychology of Persuasion," New York: HarperCollins. 2007.

[21] D. Gragg, "A Multi-Level Defense Against Social Engineering," SANS Institute – InfoSec Reading Room, Tech. Rep. 2003.

[22] F. Stajano and P. Wilson, "Understanding Scam Victims: Seven Principles for Systems Security," *Commun. ACM*, vol. 54, no. 3, pp. 70-75. 2011.

[23] D. Modic and S. Lea, "Scam Compliance and the Psychology of Presuasion," *SSRN Electronic Journal*, DOI: 10.2139/ssrn.2364464, pp. 1-34, 2013.

[24] T. Whitty, "The Scammers Persuasive Techniques Model Development of a Stage Model to Explain the Online Dating Romance Scam," *British Journal of Criminology*, vol. 53, no. 4, pp. 665-684, 2013.

[25] MCIT. 2017. NCSC: 26 Milion Phishing E-Mails Targetes Saudi Arabia. Available at : https://www.mcit.gov.sa/en/media-center/news/99030 [Accessed : 2/1/2021]

[26] J. Alghazo, and Z. Kazimi, "Social Engineering in Phishing Attacks in the Eastern Province of Saudi Arabia," *Asian Journal of Information Technology* , vol. 12, no. 3, pp. 91-98, 2013.

[27] L. Segovia, F. Torres, M. Rosillo, E. Tapia, F. Albarado, and D. Saltos, "Social engineering as an attack vector for ransomware" *In Proceedings of the Conference on Electrical Engineering and Information Communication Technology, IEEE*, DOI: 10.1109/CHILECON.2017.8229528, 2017.

[28] G. Mohamed, M. Mohideen, and S. Banu, "E-Mail Phishing – An open threat to everyone," *International Journal of Scientific and Research Publication*, vol. 4, no. 2, pp. 1-4, 2014.

[29] P. Pavlou and L. Chai, L. "What Drives Electronic Commerce Across Cultures? A Cross-Cultural Empirical Investigation of The Theory of Planned Behaviour," *Journal of Electronic Commerce Research*, vol. 3, no. 4, pp. 240-253, 2002.

[30] J. Rise, V. Kovac, P. Kraft and I. Moan, "Predicting the intention to quit smoking and quitting behaviour: Extending the theory of planned behaviour," *British Journal of Health Psychology*, vol. 13, no. 2, pp. 291-310, 2008.

[31] C. Wong and B. Mullen, "Predicting breakfast consumption: An application of the theory of planned behaviour and the investigation of past behaviour and executive function," *British journal of Health Psychology*, pp. 489-504, 2009.

[32] Y. Feng, "Traditional Alcohol Use Among Rural Yi Minorityin China: An Application of Theory of Planned Behaviour," *Public Access Theses and Dissertations from the College of Education and Human Sciences*, 2015.

[33] Gulf Business. 2020. Saudi Arabia led GCC in number of phishing attacks in Q2: Kaspersky report [accessed 06/02/2021]

[34] D. Aljeaid, A. Alzhrani, M. Alrougi, and O. Almalki, "Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks," *information MDPI*, vol. 11, no. 12, pp. 1-18, 2020.

[35] S. Hagger, D. Chatzisarantis, and H. Biddle, "A meta-analytic review of the theories of reasoned action and planned behaviour in physical activity: Predictive validity and the contribution of additional variables," *Journal of Sport and Exercise Psychology*, vol. 24, no. 1, pp. 3–32, 2002.

[36] T. Sommestad, H. Karlzen, and J. Hallberg, "The Theory of Planned Behaviour and Information Security Policy Compliance," *Journal of Computer Information Systems*, vol. 59, no. 4, pp. 344-353, 2019.

[37] M. Rousseau, B. Sitkin, S. Burt and C. Camerer, C. "Not so different after all: a cross-discipline view of trust," *Academy of Management Review*, vol. 23, no. 3, pp. 393-404,1998.

[38] A. Hadadgar, C. Tahereh, M. Ito, D. Zahra, M. Nahidossadat and Z. Nabil, "Applicability of the theory of planned behaviour in explaining the general practitioners eLearning use in continuing medical education" *BMC Med Educ*, vol. 16, no. 1, 2016.

[39] D. Schifter and I. Ajzen, "Intention, Perceived Control, and Weight Loss: An Application of the Theory of Planned Behaviour," *Journal of Presenality and Social Psycology*, vol. 49, no. 3, pp. 843-851, 1985.

[40] H. Huang, J. Tan and L. Liu, "Countermeasure Techniques for Deceptive Phishing Attack," *International Conference on New Trends in Information and Service Science*, *IEEE*, pp. 636–641, 2009.

[41] I. Ajzen, T. Brown and F. Carvajal, "Explaining the Discrepancy Between Intentions and Actions: The Case of Hypothetical Bias in Contingent Valuation" *PSPB*, vol. 30, no. 9, pp.1108-1121, 2004.

[42] Behavioural Change Models. 2019. The Theory of Planned Behaviour. Available at: https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behaviouralchangetheories/BehaviouralChangeTheories3.html [Accessed : 02/02/2021]

[43] N. Burns and S. Grove, "Understanding Nursing Research Building an Evidence-Based Practice, 5th edition, Maryland, Heights: Elsevier Inc, 2011.

[44] C. Armitage, and M. Conner, "Efficacy of the Theory of Planned Behaviour: A meta-analytic Review," *British Journal of Social Psychology* , vol. 40, no. 4, pp. 471-499, 2001.

[45] G. Godin and G. Kok, "The Theory of Planned Behaviour: A Review of its Applications to Health-Related Behaviours" *The Science of Health Promotion*, vol. 11, no. 2, pp. 87-98, 1996.

[46] C. Nunally, and B. Ira, "Psychometric Theory," 2nd edition. New York: McGraw-Hill, Inc., 1978.

[47] I. Ajzen, "Perceived Behavioural Control, Self-Efficacy, Locus of Control, and The Theory of Planned Behaviour," *Journal of Applied Social Psychology*, vol. 32, no. 4, pp. 665-683, 2002.

[48] P. Gavaza, C. Brown, K. Lawson, K. Rascati J. Wilson and M. Steinhardt, "Examination of Pharmacists' Intention to Report Serious Adverse Drug Events (Ades) to the FDA Using the Theory of Planned Behaviour," *Research in Social and Administrative Pharmacy*, vol. 7, no.4, pp. 369-382, 2011.

[49] G. Haktanir, "Prediction of Safety-Related Behaviour among Turkish Nurses: an Application of Theory of Planned Behaviour and Effects of Safety ClimatePerceptions," *PhD thesis*, Middle East Technical University, 2011.

[50] J. Mashburn, C. Brown, M. Shepherd, J, Wilson , J. Barner and J. Marxwell, "Using the Theory of Planned Behaviour to Predict Texas Community Pharmacists'willingness to Provide Sterile Syringes to Known or Suspected Intravenous Drug Users" *PhD thesis*, the University of Texas, 2003.

[51] L. Ghahremani, S. Niknami and M. Nazari, "The Prediction of Physical Activity Intention and Behaviour in Elderly Male Residents of A Nursing Home: A Comparison of Two Behavioural Theories," *Iranian journal of medical sciences*, vol. 37, no. 1, pp. 23-31, 2012.

[52] Z. Jie, B. Reithel, and L. Han, "Impact of Perceived Technical Protection on Security Behaviours," *Information Management and Computer Security*, vol. 17, no. 4, pp. 330-340, 2009.

[53] N. Ko, S. Yeh, S. Tsay, H. Ma, C. Chen, S. Pan, M. Feng, M. Chiang, Y. Lee, L. Chang and J. Jang, "Intention to Comply with Post-Exposure Management among Nurses Exposed to Blood and Body Fluids in Taiwan: Application of the Theory of Planned Behaviour" *Journal of Hospital Infection*, vol. 77, no. 4, pp. 321-326, 2011.

[54] H. Edwards, R. Nash, J. Najman, P. Yates, B. Fentiman, A. Dewar, A. Walsh, J. McDowell and H. Skerman, "Determinants of Nurses' Intention to Administer Opioids for Pain Relief," *Nursing and Health Sciences*, vol. 3, no. 3, pp. 149-159, 2001.

[55] T. Kortteisto, M. Kaila, J. Komulainen, T. Mäntyranta and P. Rissanen, "Research Article Healthcare Professionals' Intentions to Use Clinical Guidelines: A Survey using the Theory of Planned Behaviour," *Implementation Science*, vol. 5, no.1, 2010.

[56] D. Polit and C. Beck, "Nursing research: principles and methods," 7th edition. Philadelphia: Lippincott Williams & Wilkins, 2004.

[57] I. Ajzen, and M. Fishbein, "Understanding Attitudes and Predicting Social Behaviour," Englewood Cliffs, NJ: Prentice-Hall, 1980.

[58] Hofstede Insight. 2020. Country Comparison. Available Online : https://www.hofstede-insights.com/country-comparison/ (Accessed : 15/12/2020)

[59] M. Najafi, A. Ardalan, A. Akbarisari, A. Noorbala and H. Elmi, "Theory of Planned Behvior and Disaster Preparedness" *PLOS*, 2017.

[60] I, Ajzen, "Constructing a Theory of Planned Behaviour questionnaire" [Online]. Available: http://www.people.umass.edu/aizen

[61] I. Ajzen, "The theory of planned behaviour," *Organizational Behaviour and Human Decision Processes*, vol. 50, pp. 179-211, 1991.

[62] C. Anne, F. Christophe, D. Pierre and J. John, "Web Site spill over to email campaign: The role of privacy, trust and shoppers' attitudes," *Journal of Business Research*, vol. 63, no. 9, pp. 993-999, 2010.

[63] S. Hamidreza, K. Farzan, and R. Mona, "Employees' Behaviour in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter?," *Journal of Computer Information Systems*, pp. 1-12, 2020.

[64] K. Alqasa, I. Filzah, O. Siti, and Z. Ali, "The impact of students' attitude and subjective norm on the behavioural intention to use services of banking system," *Interational Journal Business Information Systems*, vol. 15, no. 1, pp. 105-122, 2014.

[65] T. Yang, "The decision behaviour of facebook users," *The Journal of Computer Information Systems*, vol. 52, no. 3, pp.50–59, 2012.

[66] S. Nader, S. Mehdi, S. Rossouw, F. Steven, A. Norijihan and H. Tutut, "Information security conscious care behaviour formation in organizations," *Computer and Secuirty*, vol. 53, pp. 65-78, 2015.

[67] G. Joey, "The theory of planned behaviour and Internet purchasing", *Emerald*, vol. 14, no. 3, pp. 198-212, 2004.