A CONCEPTUAL FRAMEWORK FOR SMARTPHONE SECURITY AMONG ARAB MILLENNIALS

Mahmood Hussain Shah
School of Strategy and Leadership, Coventry University, Coventry, UK
Email: ac3559@coventry.ac.uk
Nisreen Ameen
School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK
Email: n.ameen@qmul.ac.uk

Abstract

The rapid growth of smartphone adoption and use in the Middle East has led to some critical post-adoption issues, including ensuring that smartphones are used securely. Moreover, there is a gap in the existing literature on the perceptions and behaviour of individual consumers, especially millennials, in relation to mobile security and dealing with smartphone security threats. Little research on this subject has been carried out in developing countries, particularly in the Middle East, in a cross-national context. Therefore, this research aims to analyse the factors that can affect smartphone security behaviour among millennials in a cross-national context in the Middle East. The model developed in this research is based on a combination of the protection motivation theory (PMT) and the extended unified theory of acceptance and use of technology (UTAUT2), with additional factors specifically related to millennials' smartphone security behaviour in the Middle East. The initial findings indicate that (1) there is a gap in research on the security behaviour of Arab millennials, despite the existence of serious security threats associated with their use of these technologies; and (2) there is a gap in research on similarities and differences in smartphone security behaviour among consumers in a cross-national context. A questionnaire will be distributed online to consumers who are 18–29 years old in Iraq, Jordan and the UAE. This is the first research to study millennial Arabs' security behaviour around smartphones and mobile applications in a cross- national context. In addition, the conceptual framework proposed in this research combines the PMT and the UTAUT2, with a further extension via the inclusion of three additional factors: privacy concerns; security threats related to smartphone-specific characteristics; and cybersecurity acculturation. Furthermore, this research bridges the gap in knowledge in terms of addressing the lack of research on millennials smartphone users in the Middle East region as they form the largest segment of the population.

Keywords Smartphone security behaviour, Middle East, UTAUT2, PMT, Arab culture

1. INTRODUCTION

With the growing use of smartphones and mobile applications, there is a need to protect consumers' data to ensure that people continue to use these technologies safely. It is anticipated that by 2020, almost three-quarters of the global population will benefit from a mobile subscription (GSMA, 2017). The individual mobile user is able to access various mobile services, such as m-health, m-learning, m-commerce, m-money and m-banking. Given the sensitivity of the information provided and used by individuals on smartphones, it is important to study issues related to data protection and cybersecurity attacks. The number of fraud attempts made through mobile channels is dramatically increasing (O'Driscoll, 2018) and these attempts are expected to continue evolving (Cybersecurity Ventures, 2017). In 2017, mobile applications were downloaded a total of 197 billion times (Statista, 2018). The high use of smartphones, along with the large amount of valuable and private information they hold, makes them attractive to attackers who are interested in exploiting the devices to obtain private information (Bitten et al., 2018). One of the most challenging trends in mobile security is that individuals do not fully understand the risks inherent in using mobile devices. Mobile applications are widely varied and often poorly understood, particularly their actions and functions related to privacy and security

(Shah, 2013). Users of smartphone devices play an important role in ensuring information is kept secure when using smartphones. These vulnerable devices can jeopardise the confidentiality, integrity and availability of individuals' sensitive data. While smartphones offer huge opportunities for positive experiences, threats to users' security and privacy emerge at the same time. Those include malicious apps, data loss, surveillance and profiling, to name just a few (Okeke and Shah, 2016; Kraus et al., 2017). As a high number of mobile applications are available freely, mobile users often use them without paying attention to the security aspects.

Young Arabs aged 18–29 years (*millennials*) are active users of smartphones and mobile applications (Ameen et al., 2018a; Ameen and Willis, 2018a; Ameen and Willis, 2018b). In fact, they are the most engaged consumers in using new technologies. The security threats for this particular age group are more serious than for the other age groups. Hence, studying their behaviour in terms of ensuring the secure use of smartphones and mobile applications is important. Moreover, this particular segment of smartphone users can influence the security behaviour of other (younger or older) consumers. Despite the fact that the literature is rich in studies of online security behaviour, little is known about the context of perceptions and behaviour relating to mobile security among individual consumers in developing countries. In addition, there is inadequate research about ***millennials'*** behaviour in dealing with mobile (smartphone) security threats, particularly in the Middle East in a cross-national context. In order to bridge this gap, this research develops a theoretical model on consumers' protective behaviour in relation to mobile security threats. Hence, the main aim of this research is to analyse the factors that can affect smartphone security behaviour among ***millennials*** in a cross-national context in the Middle East.

This research contributes to the existing knowledge in terms of both theory and practice. First, this is the first research that studies young Arabs' security behaviour around smartphones and mobile applications in a cross-national context. Second, the conceptual framework proposed in this research combines the extended unified theory of acceptance and use of technology (UTAUT2) and the protection motivation theory (PMT), with a further extension via the inclusion of three additional factors: privacy concerns; smartphone-specific features security threats; and cybersecurity acculturation. Third, the research bridges the knowledge gap by addressing the lack of research on young smartphone users in the Middle East region, who form the largest segment of the population in the region. In addition, the research highlights important aspects related to smartphone security behaviour among ***millennials*** in the Middle East, which has important implications for policy makers in the region in terms of policy- making and developing new training programmes targeted at young smartphone consumers in the region.

2. LITERATURE REVIEW

2.1 Smartphone security threats in the Middle East

As their use increases, mobile internet in the Middle East and e-commerce transactions are becoming major targets for cybercriminals (Aboul-Enein, 2017). The smartphone penetration rate is increasing rapidly in the region, ranging from 30% in some Arab countries to 99% in the UAE (Statista, 2017). The extensive and rapid penetration of smartphones and the mobile internet is attracting cyber criminals, leading to a rapid increase in the number of attempted cybercrime in the region (Radcliffe and Sink, 2018).

The Middle East is considered at a high security risk in terms of cybersecurity due to many factors related to technology, people, governance and processes (PWC, 2016). The PWC 2016 report explains that companies in the Middle East are relying heavily on technology to fix cybersecurity issues, while the real concern is human error. Previous studies explained that

smartphones pose major cybersecurity threats due to the large amount of sensitive data that can be gathered through the use of mobile internet and mobile applications (O'Driscoll, 2018). Bitton et al. (2018) categorised mobile security into four main areas of focus: mobile applications (application installation and application handling); browsing and communication (browser, virtual communication and accounts); communication channels (networks and physical channels); and devices (operating system, data privacy and security systems). There are many types of mobile attacks that individuals may encounter. Examples include the following: phishing attacks (via e-mail, websites, forums and social network fraud, such as fake links, friend or game requests); application attacks (notifications, such as error messages, in-app pop-ups, malicious advertisements, clicking fraud, trojan applications and rootkits); and weak authentication attacks (due to password-cracking, password reuse, default passwords, and no screen lock) (Bitton et al., 2018).

The extant literature highlighted the importance of human security behaviour (e.g. Hui et al., 2017; Venkatesh et al., 2017; Moody et al., 2018). While the majority of previous research focused on individuals' online security (e.g. Choi et al., 2018; Gratian et al., 2018; McCormac et al., 2017), only a limited number of studies have focused on the socio-cognitive behaviours that affect mobile security practices and security behaviour (e.g. Allam et al., 2014; Masrek et al. 2017; Ophoff and Robinson, 2014). The skills required from a mobile user to interact safely with his or her smartphone are different from those that are required for safe and responsible PC use (Bitton et al., 2018). Compared with desktop users, mobile device users are at least three times more vulnerable to phishing attacks (Kessem, 2012). Some of the reasons for this vulnerability are small screen size, lack of identity indicators, inconvenience of user input, switching between applications, and the habits and preferences of mobile device users. Hence, studying the behaviour of mobile users is essential (Goel and Jain, 2018).

2.2 Cybersecurity behaviour theories

The existing literature is rich with theories used to study individuals' security behaviour. These include the PMT (Rogers, 1975; 1983; Maddux and Rogers, 1983), general deterrence theory (Gibbs 1975), rational choice theory (Becker, 1968), neutralisation theory (Sykes and Matza, 1957), the theory of reasoned action (Fishbein and Ajzen, 1975; Ajzen and Fishbein, 1980), the theory of planned behaviour (Ajzen, 1985; 1991), social cognitive theory (Bandura, 1986) and social learning theory (Miller and Dollard, 1941). However, these theories focused on the behaviour of employees in an organisational context rather than on consumers in a voluntary setting.

The PMT was developed by Rogers (1975; 1983) and Maddux and Rogers (1983). The theory stems from both the threat appraisal and the coping appraisal. The theory has been applied in the context of employee awareness of organisational policies on information security (Herath and Rao, 2009; Siponen et al., 2010) and individual use of security software (Johnston and Warkentin, 2010). However, the application of this theory in the context of ***millennials'*** smartphone security behaviour in a voluntary setting is limited. The theory integrated four main factors: perceived risk vulnerability; severity of the adverse consequences; perceived response efficacy; and response cost (Rogers, 1975; 1983; Maddux and Rogers, 1983). Table 1 shows examples of the most recent studies that used or extended the PMT in the area of cybersecurity behaviour.

Table 1. Examples of most recent studies that used or extended the PMT

Author(s)	Country	Context	Methodology	Findings
Tsai et al. (2016)	United States	Amazon Mechanical Turk (MTurk)	An online survey was used to collect data. 988 usable responses were used in the work.	Coping appraisal variables were the strongest predictors of online safety intentions, especially habit strength, response efficacy, and personal responsibility. Threat severity was also a significant predictor.
Boss et al. (2015)	United States	Operating System environment	A field experiment was used in this study. 125 students participated in study 1. 327 students participated in study 2.	Fear and maladaptive rewards play a significant role in determining protection motivation.
Dang-Pham And Pittayachawan (2015)	Australia	Avoiding malware in Bring Your Own Device in a university Setting	A questionnaire was used. 252 usable responses were used in the analysis.	Intention to perform malware avoidance behaviour differed across the contexts. Furthermore, perceptions of self-efficacy and vulnerability had different impacts on such intention and other variables in the model.
Moody et al. (2018)	Finland	Security systems in organisations	A questionnaire was used. 274 usable responses were used for study 1. 393 usable responses were used in study 2.	Response efficacy, threat, habit, role values, fear, neutralisation and reactance are important factors for information systems security.
Gao et al. (2018)	China	Smartphone-based social network service (SNS)	An online survey was used. 528 usable responses were used in the analysis.	Ubiquitous connectivity could increase SNS users' discontinuous usage intention though raising privacy concerns and protection motivation, and through aggravating their information overload and SNS exhaustion.
Jansen and van Schaik (2018)	General internet users	Phishing attacks on the internet	A pre-test post-test design was used. In the pre-test, 1,201 internet users filled out an online survey. In the post-test, data were collected from 786 internet users.	The study found that PMT model relations hold in the domain of phishing. Self-efficacy and fear were the most important predictors of protection motivation.

The first version of UTAUT was developed by Venkatesh et al. (2003). The authors found similarities among the constructs used in previous theories. The model was built by comparing and testing eight main technology acceptance theories: the theory of reasoned action (Fishbein and Ajzen, 1975; Ajzen and Fishbein, 1980), the technology acceptance model (TAM) (Davis, 1989), the motivational model, the theory of planned behaviour (TPB) (Ajzen, 1985; 1991), the

combined TAM and TPB (Taylor and Todd, 1995), the model of PC utilisation (Thompson et al., 1994), diffusion of innovation theory (Rogers, 2003) and social cognitive theory (Bandura, 1986). The extended UTAUT (Venkatesh et al., 2012) was an extension of this theory fit the context of consumers' adoption and use of technology in a voluntary setting. The model integrated the factors: performance expectancy, effort expectancy, social influence, facilitating conditions, price value, habit, behavioural intention and actual use. The theory has been used to study the adoption of different technologies in different contexts including cybersecurity behaviour (Bikoro et al., 2018). Table 2 shows examples of the most recent and relevant studies in the context of mobile cybersecurity behaviour.

Table 2. Examples of most recent studies on smartphone cybersecurity behaviour in the Middle East

Author(s)	Country	Context	Methodology	Findings
Baabdullah et al. (2015)	Saudi Arabia	Mobile government	Questionnaires were distributed in three cities in Saudi Arabia. 418 usable responses were included in the analysis.	Perceived risk is an important factor determining the use of mobile government. Personal identification numbers (PINs) do not provide very high security because they can be guessed.
Alasmari (2017)	Saudi Arabia	Mobile learning	1,203 usable responses from questionnaires were included in the quantitative analysis.	Security and privacy of online learning are important to motivate students to use the online platform. These two factors were major influences affecting students' use of the e-learning platform.
Alalawan et al. (2017)	Jordan	Mobile banking	Questionnaires were completed by participants. 343 usable responses were included in the analysis.	Trust and perceived risk are major factors affecting customers' use of mobile banking. In addition, the security issues associated with mobile banking are more complicated than online banking.
Alkhaldi (2017)	Saudi Arabia	Mobile banking	Questionnaires were completed by banking customers in Saudi Arabia. 389 usable responses were included in the analysis.	Though banks should use SMS banking, e-mails, brochures, and social networks to raise users' awareness of mobile banking services, such efforts do not help reduce consumers' perceptions of risk in using mobile banking. Banks should provide adequate protection from privacy violations.
Baabdullah (2018)	Saudi Arabia	Mobile social network games	A total of 386 questionnaires were used in the analysis.	Trust is an important factor affecting consumers' use of mobile social games. Consumers are concerned about the security of their information when using these games.

Ramadan and Aita (2018)	Syria	Mobile payment usage	A mixed-method approach was adopted, using both qualitative and quantitative data. For the quantitative part, a total of 306 usable responses were included in the analysis.	Reliability, responsiveness and security were major factors affecting the use of mobile payments. The authors described security concerns as highly emotional.
Alomari (2018)	Jordan	Mobile government	The paper was theoretical.	The use of mobile government depends on two types of trust. First, trust in the internet. Second, trust in the government and how it uses data.
Mutahar et al. (2018)	Yemen	Mobile banking	482 usable responses were included in the analysis.	Perceived risk is categorised into five main categories: privacy risk, financial risk, time risk, psychological risk and security risk.

The results of these studies highlighted the significance of ensuring the security of the systems they focused on. The results in table 2 reveal a number of gaps in the existing literature. First, there is a lack of research on smartphone cybersecurity behaviour among ***millennials*** in the Middle East in a voluntary setting. Second, there is research gap on smartphone security behaviour in a cross-national context in the Middle East. Third, the majority of previous studies focused on cybersecurity behaviour in the areas of mobile banking, financial services and mobile government, despite the fact that security threats are not limited to these technologies. Fourth, there is a lack of research focusing on aspects related to culture (namely, acculturation, specifically cybersecurity acculturation) and smartphone-specific security features. Previous studies highlighted the significant role of acculturation in the use of technology, specifically in developing and emerging countries (Straub et al., 2001; Loch et al., 2003). Hence, acculturation can also play a significant role in smartphone security behaviour. In addition, Tu and Yuan (2015) explained that wireless devices, including smartphones, have specific features that bring new security risks to organisations. Hence, the features specific to smartphones can lead to increased risk for individuals.

3 CONCEPTUAL FRAMEWORK

The model proposed in the present study combines the main constructs of the UTAUT2 and the constructs from the PMT. The constructs of the UTAUT2 are as follows: effort expectancy; habit; price value; facilitating conditions; social influence; hedonic motivation; and behavioural intention (measurement items adapted from Venkatesh et al. (2012)). The constructs from the PMT are as follows: perceived risk vulnerability; severity of the adverse consequences; perceived response efficacy; and response cost (measurement items adapted from studies by Woon et al. (2005), Thompson et al. (2017) and Verkijika (2018)). In addition, three new factors that were found to be important in the case of mobile phone security have been integrated: cybersecurity acculturation (measurement items adapted from Straub et al. (2001) and Ameen and Willis (2018a)); privacy concerns (measurement items adapted from Dinev and Hart (2004, 2006)) and smartphone-specific features security threats (measurement items adapted from Tu and Yuan (2015), Dimensional Research (2017) and Becher and Freiling

(2011)). Some items have been added by the authors to fit the context of mobile security in the Middle East. The factors integrated in the model and the proposed hypotheses for their significance are discussed in the following sections.

3.1 Acculturation (cybersecurity acculturation)

Cybersecurity acculturation refers to inculcating best practices, good habits and behaviours on good and safe use of smartphones (Hashim, 2011). Previous studies emphasised the significance of acculturation: when smartphone users travel to more technologically advanced countries, this influences their use of the device and its mobile applications (Ameen and Willis, 2018a). It also refers to national strategy for cybersecurity acculturation and capacity building programmes (NACSA, 2018). The Middle East lags behind more developed regions in terms of security awareness (Aboul-Enein, 2017). Therefore, cybersecurity acculturation can have a significant effect on ***millennials'*** behavioural intention towards their actual security behaviour. Thus:

H1. *Cybersecurity acculturation will have a significant positive effect on behavioural intention towards smartphone security behaviour.*

3.2 Perceived vulnerability

Perceived vulnerability refers to one's perception of experiencing possible negative consequences of performing a risky behaviour (Rogers, 1983; Salleh et al., 2012). Crossler (2010) describes perceived vulnerability as the personal probability or likelihood of a security incident occurring and defines perceived severity as the impact of consequences resulting from a security incident. As ***millennials*** in the Middle East use smartphones and mobile applications frequently (Ameen et al., 2018a; Ameen et al., 2018b), their perceptions regarding the probability of encountering a security attack increase. Thus, it is hypothesised:

H2. *Perceived vulnerability will have a significant positive effect on behavioural intention towards smartphone security behaviour.*

3.3 Severity of adverse consequences

Perceived severity of adverse consequences refers to one's perception of the level of damage that may result from engaging in a risky situation (Rogers, 1983; Salleh et al., 2012). For a young user of smartphones and mobile applications, it is important to understand the consequences of any security negligence when using a smartphone. Hence, perceived severity of adverse consequences can have a strong effect on behavioural intention. Thus, it is hypothesised:

H3. *Perceived severity of adverse consequences will have a significant positive effect on behavioural intention towards smartphone security behaviour.*

3.4 Perceived response efficacy

Perceived response efficacy refers to the degree to which an individual believes that the response one takes is effective in alleviating the threat (Rogers, 1983; La Rose et al., 2006). The inclusion of response efficacy in any fear-appeal communication is of the utmost importance (La Rose et al., 2006). Security response efficacy means the beliefs regarding

whether the recommended preventive response will be effective in avoiding or reducing security threats. For example, anti-virus software has been reported as an effective and efficient solution for detecting and preventing virus threats. Thus, a young smartphone user in an Arab country can assume that installing anti-virus software will provide the mobile user with confidence that this solution will prevent or mitigate the security threat (Al-Ghaith, 2016). Therefore, it is hypothesised:

H4. *Perceived response efficacy will have a significant positive effect on behavioural intention towards smartphone security behaviour.*

3.5 Response cost

Response cost refers to the cost of performing the recommended behaviour (Rogers, 1983). Response cost negatively influences individuals' intention to adopt adaptive behaviours. For a young smartphone consumer in the Middle East, response cost can have a negative effect on behavioural intention towards smartphone security behaviour. Thus:

H5. *Response cost will have a significant negative effect on behavioural intention towards smartphone security behaviour.*

3.6 Privacy concerns

This factor refers to the individual's privacy concerns, which have been highlighted in previous studies (e.g. Lian and Lin 2008; Sims and Xu, 2012; Tucker, 2014; Krafft et al., 2017). A recent GDPR report showed that consumers are becoming concerned about their privacy when using mobile applications (GDPR, 2018). However, consumers are not acting on their privacy concerns when using mobile applications (GDPR, 2018). The situation is similar in the Middle East (Al-Ghaith, 2016), as consumers do not check the permissions of their pre-installed mobile apps on their Android or iOS devices. Thus:

H6. *Privacy concerns will have a significant negative effect on behavioural intention towards smartphone security behaviour.*

3.7 Smartphone-specific features security threats

Previous studies highlighted that the threats associated with the use of smartphones exceed those associated with the use of desktop computers (Tu and Yuan, 2015; Al-Ghaith, 2016). This is due to features that are specific to smartphones, such as the risk of physically losing the device, the ability to connect to different networks, the use of different mobile applications, data breaches, the mixed use of smartphones for personal and business purposes, the use of free mobile apps that share personal information, the ability to make payments through the device, the battery life, the integrated camera, and the integration of mobile messaging apps (e.g., Viber, Skype and WhatsApp). Thus, it is hypothesised:

H7. *Smartphone-specific features security threats will have a significant negative effect on behavioural intention towards smartphone security behaviour.*

3.8 Performance expectancy

Performance expectancy refers to "the degree to which using a technology will provide benefits to consumers in performing certain activities" (Venkatesh et al., 2012). This factor was significant in previous studies related to the use of smartphones and mobile applications (Ameen et al., 2018a; Ameen and Willis, 2018a). Understanding the benefits of ensuring the security of a smartphone and its mobile applications can have a significant positive effect on behavioural intention. Thus:

H8. *Performance expectancy will have a significant positive effect on behavioural intention towards smartphone security behaviour.*

3.9 Effort expectancy

Effort expectancy refers to "the degree of ease associated with consumers' use of technology" (Venkatesh et al., 2012). Effort expectancy is an important antecedent to behavioural intention towards security behaviour when using different technologies (Iskandar, 2017). The easier the methods used to ensure that the smartphone is secure, the more likely it is that the individual user will ensure its security. Therefore:

H9. *Effort expectancy will have a significant positive effect on behavioural intention towards smartphone security behaviour.*

3.10 Price value

Price value is defined as "consumers' cognitive trade-off between the perceived benefits of the applications and the monetary cost for using them" (Venkatesh et al., 2012). This factor refers to consumers' evaluation of the cost associated with ensuring the security of their smartphones in comparison with the benefits of doing so. If the benefits of security outweigh the cost, price value will be positive (Ameen et al., 2018a). However, the price of anti-virus and smartphone security for Android and Apple iOS may be considered high by some consumers. Thus:

H10. *Price value will have a significant positive effect on behavioural intention towards smartphone security behaviour.*

3.11 Habit

Limayem et al. (2007) define habit as "the extent to which people tend to perform behaviours automatically because of learning". Venkatesh et al. (2012) emphasised the importance of habit as a predictor of both behavioural intention and actual use of technology. Given that the Middle East generally lags behind in terms of cybersecurity behaviour with regard to mobile phones and other technologies (Aboul-Enein, 2017), smartphone users may not have developed strong habits related to the security of their smartphones and mobile applications. Thus:

H11. *Habit will have an insignificant positive effect on behavioural intention towards smartphone security behaviour.*

H12. *Habit will have an insignificant positive effect on actual smartphone security behaviour.*

3.12 Social influence

Social influence refers to "the extent to which consumers perceive that important others (e.g., family and friends) believe they should use a particular technology" (Venkatesh et al., 2012). The influence of friends and family members can have a significant impact on keeping one's smartphone and mobile applications secure (Das, 2014). There is a contradiction in the existing literature in terms of the significance of social influence: while earlier studies found that social influence has an effect on technology adoption and usage behaviour (Das, 2014), a more recent study (Ameen and Willis, 2018a) found that this factor does not have a significant effect on the use of smartphones or mobile applications in Iraq, Jordan or the United Arab Emirates. In this research, the following hypothesis is proposed:

H13. *Social influence will have a significant positive effect on behavioural intention towards smartphone security behaviour.*

3.13 Facilitating conditions

Facilitating conditions refer to "consumers' perceptions of the resources and support available to perform a behaviour" (Venkatesh et al., 2012). They represent the resources available to consumers to ensure the secure use of smartphones and mobile applications. These resources take the form of educational materials, information available to the individual, help obtained from others to aid an individual's learning on how to use technology, and whether or not ensuring the security of smartphones and mobile applications is compatible with ensuring the security of other technologies the individual is using. Hence, this factor links to compatibility and ease of use (Venkatesh et al., 2003). Thus:

H14. *Facilitating conditions will have a significant positive effect on behavioural intention towards smartphone security behaviour.*

3.14 Behavioural intention

Behavioural intention refers to the process of the individual's readiness (cognitively) to perform a certain behaviour (Ajzen and Fishbein, 1980). Accordingly, the likelihood of a person performing a certain behaviour depends on their intentions (Ajzen and Fishbein, 1980). In this study, we hypothesise that behavioural intention will have a significant effect on actual smartphone security behaviour:

H15. *Behavioural intention will have a significant positive effect on actual smartphone security behaviour.*

Figure 1 shows the research model developed in this study.

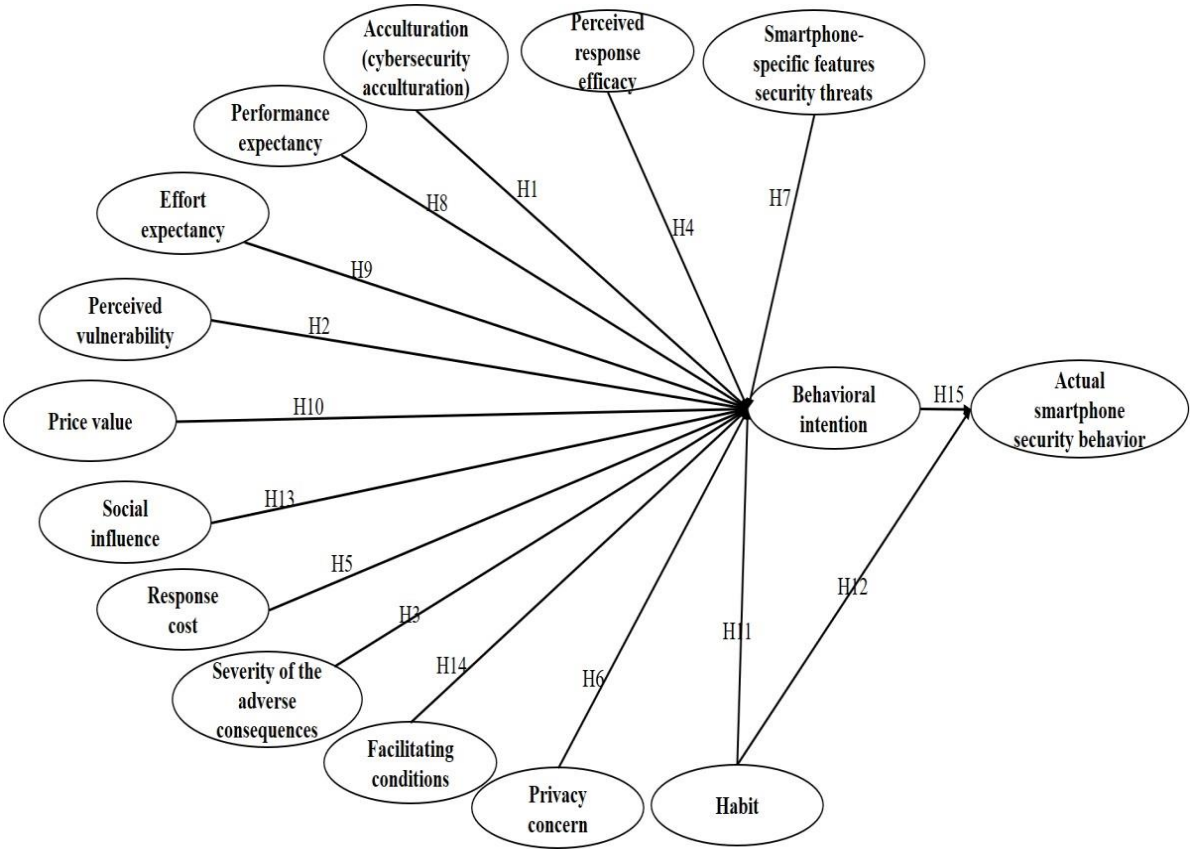

Figure. 1: Research model

4 METHODOLOGY

The research will test the model in three different Middle Eastern countries: Iraq, Jordan and the UAE. It will explore the differences between the three countries. These three countries are ranked differently in the Global Cybersecurity Index (2017): the UAE is ranked as 47th globally, while Jordan and Iraq are ranked 93rd and 159th respectively (International Telecommunication Union, 2017). We are studying the behaviour of mobile users in these three countries because they represent the exemplars of distinct contextual difference. Data will be collected from ***millennials*** in Iraq, Jordan and the UAE through an online questionnaire using random sampling. The link will be distributed through social media platforms and mobile phones (using SMS and VoIP applications such as Viber and WhatsApp) to enable participants to complete the questionnaire. The authors will endeavour to obtain a total of 533 completed questionnaires from each country from young adults aged 18–29 years. The collected data will be analysed using partial least squares-structural equation modelling (PLS-SEM). Both Statistical Package for the Social Sciences (SPSS) and SmartPLS software will be used to analyse the data.

5 INITIAL FINDINGS

This research aims to analyse the factors that can affect smartphone security behaviour among ***millennials*** in the Middle East. The review of the existing literature on mobile security revealed a

number of findings. Despite the growth of cybersecurity crimes and their threats to the security and privacy of individuals' information, there is a lack of research in this area. Previous studies identified factors such as trust, perceived risk, security and privacy as important for the use of various individual mobile applications (e.g. Alasmari, 2017; Alkhaldi, 2017; Alomari, 2018). However, there is a gap in the existing knowledge about the security behaviour of young active users of smartphones.

The conceptual framework developed in this research combines two well-known theories: the UTAUT2 (Venkatesh et al., 2012) and the PMT (Rogers, 1975, 1983; Maddux and Rogers, 1983). Existing studies used a combination of factors to study the security behaviour of individuals in voluntary and organisational settings. Nevertheless, the unique characteristics of smartphones and mobile applications make ensuring their security more challenging than ensuring the security of other technologies (Shah, 2013). Hence, it is important to integrate the factors that are specifically related to security behaviour when using smartphones. In addition, investigating the level of cybersecurity awareness and its effect (acculturation) is important in order to assess the effectiveness of cybersecurity awareness campaigns and their influence on individuals' smartphone security behaviour.

6 RESEARCH CONTRIBUTIONS AND IMPLICATIONS

This research will contribute to the existing knowledge in terms of both theory and practice. First, this is the first research to study young people's security behaviour with regard to smartphones and mobile applications in a cross-national context in the Middle East. Second, the conceptual framework proposed in this research combines the UTAUT2 and the PMT, with a further extension via the inclusion of three additional factors: privacy concerns; smartphone-specific features security threats; and cybersecurity acculturation. Third, the research will bridge the knowledge gap in terms of addressing the lack of research on young smartphone users in the Middle East region, who form the largest segment of the population.

In terms of the practical contributions, it is anticipated that the results of this research will help to identify new issues in terms of policy-making and the development of new training programmes related to smartphone cybersecurity in the Middle East, as the research is cross-national. Indeed, the development of more effective policies and the enhancement of a more cybersecurity-aware culture in the Middle East are expected to be two major practical contributions made by this research.

7 CONCLUSIONS, LIMITATIONS AND FUTURE RESEARCH

A conceptual framework was developed in this research to identify and examine the potential factors that affect Arab ***millennials***' security behaviour when using smartphones and mobile applications. The initial findings, based on a review of the existing literature, indicate that there is a gap in this area of research. Hence, this study proposes a new conceptual framework that integrates the PMT and the UTAUT, along with other factors specific to ensuring the security of smartphones and mobile applications. Hence, once the empirical work has been completed, the study will provide both theoretical and practical contributions.

Despite the significance of this study, it has some limitations. One of the main limitations at this stage is the lack of empirical work to validate and test the proposed model among young

smartphone users in Iraq, Jordan and UAE. Data will be collected from the three countries to validate the proposed model. In addition, the model proposed in this research is complex. However, this reflects the complexity of the phenomenon of smartphone cybersecurity behaviour and cybersecurity crime committed through these devices. The findings of this research will be limited to three countries in the Middle East. Future studies can collect data from other countries to provide an empirical validation of the proposed model. In addition, future studies should investigate other factors related to the effects of culture on cybersecurity behaviour in the Middle East.

REFERENCES

Aboul-Enein, S. (2017) Cybersecurity challenges in the Middle East. Retrieved from file:///C:/Users/User/Downloads/GP%202%20-%20S.%20ABOUL-ENEIN%20-%20Cybersecurity%20-%20ELECTRONIC.pdf (Accessed 29 September 2018).

Ajzen, I. and Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, NJ: Prentice-Hall.

Ajzen, I. (1985). From intentions to actions: a theory of planned behaviour. In: J. Kuhl and J. Beckman (eds.), *Action-control: from cognition to behaviour*. Heidelberg: Springer. (pp. 11-39).

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes*, 50 (2), pp. 179–211.

Allam, S., Flowerday, S.V. and Flowerday, E. (2014). Smartphone information security awareness: a victim of operational pressures. *Computers & Security*, 42, pp. 56–65.

Alomari, M. (2018). Mobile government adoption: citizen-centric approach [online]. *Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1484&context=amcis2018 (Accessed 1 October 2018).

Ameen, N. and Willis, R. (2018a). A generalized model for smartphone adoption and use in an Arab context: a cross-country comparison. *Information Systems Management*, 35 (3), pp. 254–274.

Ameen, N. and Willis, R., (2018b). An Examination of the Role of National IT Development and Infrastructure in Models for Smartphone Adoption and Use: The Cases of Iraq, Jordan and the UAE. In *Emerging Markets from a Multidisciplinary Perspective* (pp. 161-194). Springer, Cham.

Ameen, N., Willis, R. and Shah, M.H. (2018a). An examination of the gender gap in smartphone adoption and use in Arab countries: a cross-national study. *Computers in Human Behaviour*, 89, pp. 148–162.

Ameen, N., Willis, R., Abdullah, M.N. and Shah, M., (2018b). Towards the successful integration of e-learning systems in higher education in Iraq: A student perspective. British Journal of Educational Technology. https://doi.org/10.1111/bjet.12651.

Andeme Bikoro, D.M., Fosso Wamba, S. and Kala Kamdjoug, J.R. (2018). Determinants of cybersecurity use and behavioural intention: case of the Cameroonian public administration. In A. Rocha, H. Adeli, L. Reis and S. Costanzo (eds.), *Trends and advances in information systems and technologies, WorldCIST'18 2018* (pp. 1087–1096). Springer, Cham.

Bandura, A. (1986). *Social foundations of thought and action: a social cognitive theory*. Englewood Cliffs, NJ: Prentice Hall.

Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S. and Wolf, C. (2011). Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. In: *2011 IEEE Symposium on Security and Privacy* (pp. 96–111). IEEE.

Becker, G.S. (1968). Crime and punishment: an economic approach. *Journal of Political Economy*, 76, pp. 169¬217.

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L. and Shabtai, A. (2018). Taxonomy of mobile users' security awareness. *Computers & Security*, 73, pp. 266–293.

Boss, S., Galletta, D., Lowry, P.B., Moody, G.D. and Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39 (4), pp. 837–864.

Choi, C., Ogiela, M.R. and Chen, H.C. (2018). Intelligent approaches for security technologies. *Concurrency and Computation: Practice and Experience*, 30 (3), p. e4408.

Crossler, R. and Bélanger, F. (2014). An extended perspective on individual security behaviours: protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, 45 (4), pp. 51–71.

Cyber Security Ventures (2017). Cybercrime damages $6 trillion by 2021. Retrieved from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (Accessed 15 September 2018).

Dang-Pham, D. and Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach. *Computers & Security*, 48, pp. 281–297.

Das, S., Kim, T.H.J., Dabbish, L.A. and Hong, J.I. (2014). The effect of social influence on security sensitivity. In Proc. Symposium on Usable Privacy and Security (SOUPS) (Vol. 14).

Dimensional Research (2017). The growing threat of mobile device security breaches a global

survey of security professionals. Retrieved from https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf (Accessed 5 June 2018).

Dinev, T. and Hart, P. (2004). Internet privacy concerns and their antecedents: measurement validity and a regression model. *Behaviour & Information Technology*, 23 (6), pp. 413–422.

Dinev, T. and Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17 (1), pp. 61–80.

Fishbein, M. and Ajzen, I. (1975). *Belief, attitude, intention, and behaviour: an introduction to theory and research*. Reading, Mass; Don Mills, Ontario: Addison-Wesley.

Gao, W., Liu, Z., Guo, Q. and Li, X. (2018). The dark side of ubiquitous connectivity in smartphone-based SNS: an integrated model from information perspective. *Computers in Human Behavior*, 84, pp. 185–193.

GDPR (2018). Consumers are not acting on privacy concerns when using mobile applications [online] https://gdpr.report/news/2018/07/27/consumers-are-not-acting-on-privacy-concerns-when-using-mobile-applications/ (Accessed 29 September 2018).

Gibbs, X.P. (1975). *Crime, punishment and deterrence*. New York: Elsevier.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018). Correlating human traits and cyber security behaviour intentions. *Computers & Security*, 73, pp. 345–358.

GSMA (2017). The mobile economy: Middle East and North Africa 2017. Retrieved from https://www.gsma.com/mobileeconomy/mena (Accessed 22 December 2017).

Hashim, M.S. (2011). June. Malaysia's national cybersecurity policy: the country's cyber defence initiatives. In: *2011 Second Worldwide Cybersecurity Summit (WCS)* (pp. 1–7). IEEE.

Hui, K.L., Kim, S.H. and Wang, Q.H. (2017). Cybercrime deterrence and international legislation: evidence from distributed denial of service attacks. *MIS Quarterly*, 41 (2), p. 497-523.

International Telecommunication Union (2017). Global Cybersecurity Index (GCI) 2017. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (Accessed 5 June 2018).

Iskandar, R. (2017). *Cybersecurity in consumer adoption of smart home technology*. Doctoral dissertation, Carleton University, Ottawa.

Jansen, J. and van Schaik, P. (2018). Persuading end users to act cautiously online: a fear appeals study on phishing. *Information & Computer Security*. 26 (3), pp.264-276.

Kessem, L.S. (2012). What makes phishing so successful? Retrieved from the InformationWeek website: http://www.informationweek.in/Security/12-05-08/What_makes_phishing_so_successful.aspx (Accessed 10 June 2018).

Kraus, L., Wechsung, I. and Möller, S. (2017). Psychological needs as motivators for security and privacy actions on smartphones. *Journal of Information Security and Applications*, 34, pp. 34–45.

Maddux, J.E. and Rogers, R.W. (1983). Protection motivation theory and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19, pp. 469–479.

Masrek, M.N. and Khairuddin, I.I. (2012). Trust in mobile banking adoption in Malaysia: a conceptual framework. *Journal of Mobile Technologies, Knowledge and Society*, 12, pp. 1–12.

McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T. and Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems*, 21. pp. 1–12.

Miller, N.E. and Dollard, J. (1941). *Social learning and imitation*. New Haven: Yale University Press.

Moody, G.D., Siponen, M. and Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42 (1), pp. 285–311.

NACSA (2018). National Cybersecurity Agency. [online] https://www.nacsa.gov.my/ (Accessed 29 September 2018).

O'Driscoll, A. (2018). 100+ terrifying cybercrime and cybersecurity statistics and trends. Retrieved from https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#gref (Accessed 15 September 2018).

Okeke, R. and Shah, M. (2016). *Information theft prevention: theory and practice*. Routledge. New York.

Ophoff, J. and Robinson, M. (2014). Exploring end-user smartphone security awareness within a South African context. *Information Security for South Africa*, pp. 1–7. DOI: 10.1109/ISSA.2014.6950500.

PWC (2016). A false sense of security? Cybersecurity in the Middle East. Retrieved from https://www.pwc.com/m1/en/publications/documents/middle-east-cybersecurity-survey.pdf (Accessed 1 October 2018).

Radcliffe, D., and Sink, H. (2018) Cybercrime: why can't the Middle East get to grips with the threats? [online] https://www.zdnet.com/article/cybercrime-why-cant-the-middle-east-get-to-grips-with-the-threats/ (Accessed 1 October 2018).

Ramadan, R. and Aita, J. (2018). A model of mobile payment usage among Arab consumers. *International Journal of Bank Marketing*. 36 (7), pp.1213-1234.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91, pp. 93–114.

Shah, M. (2014). *Mobile working: technologies and business strategies*. London: Routledge.

Statista (2017). Penetration rate of smartphones in the Middle East and North Africa as of March 2017, by country [online] https://www.statista.com/statistics/779558/mena-smartphone-penetration-by-country/ (Accessed 1 October 2018).

Statista (2018). Number of mobile app downloads worldwide in 2017, 2018 and 2022 (in billions). Retrieved from https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/ (Accessed 15 September 2018).

Straub, D., Loch, K. and Hill, C. (2001). Transfer of information technology to the Arab world: a test of cultural influence modeling. *Journal of Global Information Management*, 9 (4), pp. 6–28.

Sykes, G.M. and Matza, D. (1957). Techniques of neutralization: a theory of delinquency. *American Sociological Review*, 22 (6), pp. 664–670.

Thompson, N., McGill, T.J. and Wang, X. (2017). "Security begins at home": determinants of home computer and mobile device security behaviour. *Computers & Security*, 70, pp. 376–391.

Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J. and Cotten, S.R. (2016). Understanding online safety behaviors: a protection motivation theory perspective. *Computers & Security*, 59, pp. 138–150.

Tu, Z., Turel, O., Yuan, Y. and Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: an empirical examination. *Information & Management*, 52 (4), pp. 506–517.

Venkatesh, V., Aloysius, J.A., Hoehle, H. and Burton, S. (2017). Design and evaluation of auto-ID enabled shopping assistance artifacts in customers' mobile phones: two retail store laboratory experiments. *MIS Quarterly*, 41 (1), pp. 83–113.

Venkatesh, V., Thong, J., and Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36 (1), pp. 157–178.

Verkijika, S.F. (2018). Understanding smartphone security behaviours: an extension of the protection motivation theory with anticipated regret. *Computers & Security*, doi: org/10.1016/j.cose.2018.03.008.

Woon, I., Tan, G.W. and Low, R. (2005). A protection motivation theory approach to home wireless security. In: International Conference on Information Systems 2005 proceedings (p. 31). Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1237&context=icis2005 (Accessed 1 June 2018).

Wu, J.H. and Wang, S.C. (2005). What drives mobile commerce? An empirical evaluation of the revised technology acceptance model. *Information & Management*, 42 (5), pp. 719– 729.