THE EFFECTS OF PERSUASIVE TECHNOLOGY FOR INFLUENCING END-USERS' INFORMATION SECURITY AWARENESS

Mohammed Abdullah Bawazir[1]*, Murni Mahmud[1], Nurul Nuha Abdul Molok[1], Akram M Zeki[1]

[1]Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, Malaysia

**Corresponding author: bawazir333@gmail.com*

ABSTRACT: In today's digital world, information assets have grown in importance, demanding measures to ensure their protection. Ubiquitously, end-users are having trouble ensuring the security of their personal information. The human factor is a major source of vulnerability in the field of information security. Traditional techniques that can be used to influence information security awareness (ISA) remain prohibitively expensive, time-consuming, and repetitive. In light of these challenges, this study proposes persuasive technology to influence end-users' security awareness and behaviour intention. Based on our research, persuasive technology is effective in changing end-users' attitudes and behaviours. In this context, this study assesses the effectiveness of persuasive technology use for influencing end-users' ISA. In addition, this research establishes an integrated model for improving end-users' ISA by incorporating relevant literature and multiple empirically verified theories, including Fogg Behaviour Model (FBM), Protection Motivation Theory (PMT), Theory of Planned Behaviour (TPB), and Technology Acceptance Model (TAM). The integrated model has been proposed based on the main categories of FBM (motivation, ability, and trigger) to identify the effects of key factors in the persuasive technology context for influencing end-user ISA and behaviour intention. The prototype was developed by implementing the persuasive factors of the proposed model to measure the effectiveness of persuasive technology. Quantitative data from an experiment were gathered from 100 participants to validate the proposed research model using the paired sample T-test and partial least squares (PLS) to assess security awareness in the context of persuasive technology. The research findings show that using persuasive technology has a positive influence on ISA. The results also indicate the research model significantly predicts the key factors affecting security awareness and behaviour intention with respect to persuasive technology. Thus, this study suggests a model for the creation and development of a proactive and customised security awareness system. Therefore, persuasive technology, in general, has a positive effect on users' security awareness and the intention of security behaviour.

KEY WORDS: *Persuasive technology, Information Security Awareness (ISA), Information Security Policy (ISP), Information Systems Security (ISS), Behaviour Intention (BI), Prototype.*

1. INTRODUCTION

Due to the interconnected world, computer networking technologies are expanding at a rapid rate, ultimately causing the development of information systems and increasing capabilities to process, store, and transmit digital data. However, the result of continuing changes can display various concerns related to the protection of information assets. Experts believe that technology cannot completely guarantee a secure environment for information (Dhillon & Backhouse, 2000; Safa et al., 2015). As such, high levels of connectivity, substantial growth of electronic commerce, availability of advanced hacking tools, and other aspects produce challenges to information security (Hu, Hart, & Cooke, 2007). Furthermore, violations of Information Security Policies (ISPs) have demonstrated the considerable increase in information security risks and vulnerabilities that eventually lead to information security breaches (Vance, 2010).

Apart from criminal threats and system failures, human error is the main reason for insider threats in information security. It is assumed that 50% to 70% of the Information System Security (ISS) incidents are caused either directly or indirectly by human errors to comply with IS security procedures (Siponen & Vance, 2010; Vance, Siponen, & Pahnila, 2012). The IS security literature usually describes end-users as the weakest security link for errors or computer crimes; therefore, end-users' Information Security Awareness (ISA) and information security behaviour have gained growing academic attention in the past decade (Lebek, Uffen, Neumann, Hohler, & H. Breitner, 2014a; Spears & Barki, 2010). General awareness of information security and ISP is the most important aspect of ISA (Bulgurcu, Cavusoglu, & Benbasat, 2010). Furthermore, the ISA among end-users has been described as one of the critical components of an effective IS security strategy (Bulgurcu et al., 2010; D'Arcy, Hovav, & Galletta, 2009a). Studies indicate the lack of awareness of security policies and best practices among end-users is a major cause of IS security failure and its implications (Abraham, 2011). Equally important, Behaviour Intention (BI) refers to the intention to comply with ISPs (Al-Omari, El-Gayar, & Deokar, 2012a; Bulgurcu et al., 2010). Increased ISA among end-users has a positive influence on behaviour intention to comply with ISPs.

Information security violations can have serious consequences. Loss or theft of sensitive digital information will cost financial damage and tarnish the reputation of the organization. Certainly, end-users are expected to comply with the prescribed policy. Nevertheless, end-users may encounter difficulties in complying with the information security policy (Busch et al., 2015). However, neither technology nor human approaches such as security education, training, and awareness programmes (SETA), was truly successful when implemented in silos. This is because, end-users know how to avoid technical solutions and SETA programmes can be intrusive, time-consuming and costly. Additionally, SETA programmes are not specific to the context of information security violations, have short-term effects only, or must be repeated to have long-term effects (Busch, Wolkerstorfer, Hochleitner, & Tscheligi, 2014). Hence, changing end-users' ISA and behaviour intention to comply with ISPs is considered a difficult and challenging aspect of computer security practices (Yeo, Rahim, & Ren, 2008).

Persuasive technology can be an effective approach for changing attitudes and learning purposes in terms of raising awareness on certain issues (Dolhalit, Abdul Salam, & Abdul Mutalib, 2015; Fogg, 2002). It has been applied in many fields, including marketing, health, environmental, education and other areas and has been very successful in changing people's attitudes and behaviours (Bawazir, Mahmud, Abdul Molok, & Ibrahim, 2016; Preece, 2010). Accordingly, based on the principles of persuasive technology, a system designed to promote end-user's positive awareness of information security to help them create the recommended informed security actions and enhance safe working practices can be a subjective norm to establish long-term sustainability of end-users' ISA security best practices (Bawazir et al., 2016).

The overall objective of this paper is to make three contributions. First, it seeks to identify the factors that apply in the persuasive technology context to influence end-users' ISA and security practices. These factors were adopted from the theories that have been used to explain end-users security in terms of awareness and behaviour. In addition, the proposed model is presented in this study that captures the key factors that influence the end-users' ISA. The derived hypotheses were investigated. Second, a prototype was developed to investigate the effects of persuasive technology for influencing end-users ISA. Third, the integrated model was validated to determine the positive relationship between motivation, ability and trigger factors with ISA and intention to comply with ISPs using persuasive technology.

2. REVIEW OF RELATED THEORIES

2.1. Technology Acceptance Model

Davis (1989) implemented the Technology Acceptance Model (TAM), which is a common theory of behaviour that refers to a person's decision to adopt innovations of technology based on his or her attitude. This attitude is often generated by the perceived usefulness and ease of use of the technology. Perceived usefulness is "the degree to which a person believes that the use of a system may improve his overall performance in the workplace," while perceived ease of use indicates "the extent to which a person believes the use of a system would be free of effort." In the ISS field, TAM is often used to describe the acceptance of ISS technologies or countermeasures such as ISPs. Perceived usefulness is the extent to which an end-user believes that utilising ISPs' roles and responsibilities for the protection of the information technology resources will improve their work performance. Ease of use refers to the extent to which an end-user believes that implementing ISPs and performing associated tasks and responsibilities is relatively easy and simple (Al-Omari, El-Gayar, & Deokar, 2012b; M. T. Siponen, 2000a).

2.2 Theory of Planned Behaviour

The Theory Of Planned Behaviour (TPB) (Ajzen, 1991) is one of the most relevant and often cited frameworks for the prediction of intentional behaviour in a wide variety of fields of research. The theory is based on the idea that actual behaviour is logical and results from the intention of a person to carry out the associated behaviour. Although intention does not replace actual behaviour, it represents a considerable variance in real behaviour as a strong motivation determinant. Based on TPB, the intention is derived from the three belief-based behaviour: subjective norms, perceived behavioural control and attitude towards the behaviour. This attitude results in beliefs on the effect of behaviour, the subjective norm is affected by normative beliefs (from others) and perceived behavioural control refers to control beliefs and perceived difficulty or ease of conduct behaviour. In ISS practices, normative belief may emerge from an ISS norm, culture or obligation for the responsibility, such as regulations and guidelines for protection. Following safety guidelines should have beneficial results to improve an individual's attitude about ISS. Finally, the ability and skill to conduct compliant ISS should be learned and improved to increase the perceived behavioural control (Siponen, 2000a).

2.3 Protection Motivation Theory

Rogers (1983) developed the Protection Motivation Theory (PMT), which is a well-validated theoretical framework that allows individuals to consider why they perform prescribed actions to avoid the effects of certain risks (i.e. the use of condoms to prevent the spread of HIV or not to smoke to prevent lung cancer). PMT claims that protection motivation, i.e., intention to conduct prescribed actions, is shaped by two cognitive appraisal processes arising from different appeals for fear: threat appraisal and coping response appraisal. Threat appraisal is based on the fear of a person on the perceived severity of the threat (threat-related harm) and perceived vulnerability to the threat. The coping appraisal is based on the belief that the recommended behaviour is effective in reducing the threat (response effectiveness) and that one is capable of performing the recommended behaviour (self-efficacy). However, PMT is used frequently by these concepts in ISS research to describe the motivation of end-users to comply with ISPs and to use ISS countermeasures.

2.4 Persuasive Technology - Fogg Behaviour Model (FBM)

Persuasive technology is a field of human-computer interaction (HCI) and defined as an interactive computer system that changes a person’s attitudes or behaviours, and this phenomenon is called “captology” (Fogg, 1998). Nevertheless, true persuasion entails the intention to change behaviours or habits; in other words, persuasion requires intentionality. Persuasive technologies are ubiquitous, and technology is a particularly powerful tool that allows persuasive approaches to be interactive rather than one-way (Qudaih, Bawazir, Usman, & Ibrahim, 2014). Consequently, our way of thinking and doing actions has been influenced by the digital products around us. Internet services, mobile devices, desktop computers and video games are recognised as interactive computer technology that focuses on persuasive technology research (Yu, 2012). Persuasive technology is an extremely active multidisciplinary research field focusing on the development, design and evaluation of collaborative technologies aimed at changing the awareness and actions of end-users and social influences without any kind of coercion or deception (Bawazir, Mahmud, & Abdul Molok, 2019).

Nonetheless, persuasive technologies can play a critical role in raising end-users’ awareness of information security. End-users constantly face challenges with security issues, and thus, they need persuasion to increase ISA and BI (Qudaih et al., 2014). In addition, researchers believe that users’ attitude towards the security of information needs to be changed. An increasing number of information technology systems and programmes for persuasive purposes, i.e. to change attitudes or behaviour of the users or both have been proposed (Oinas-Kukkonen & Harjumaa, 2008b). Persuasive technology is ready to help users improve their awareness and behaviour intention to be successfully targeted security behaviour (Wolmarans, 2003). Yeo et al. (2008) assert that the web-based programme has a very strong effect to improve users’ attitudes toward email management, password management and virus protection. The findings of the study also indicate that persuasive technology has improved users’ security-aware behaviour.

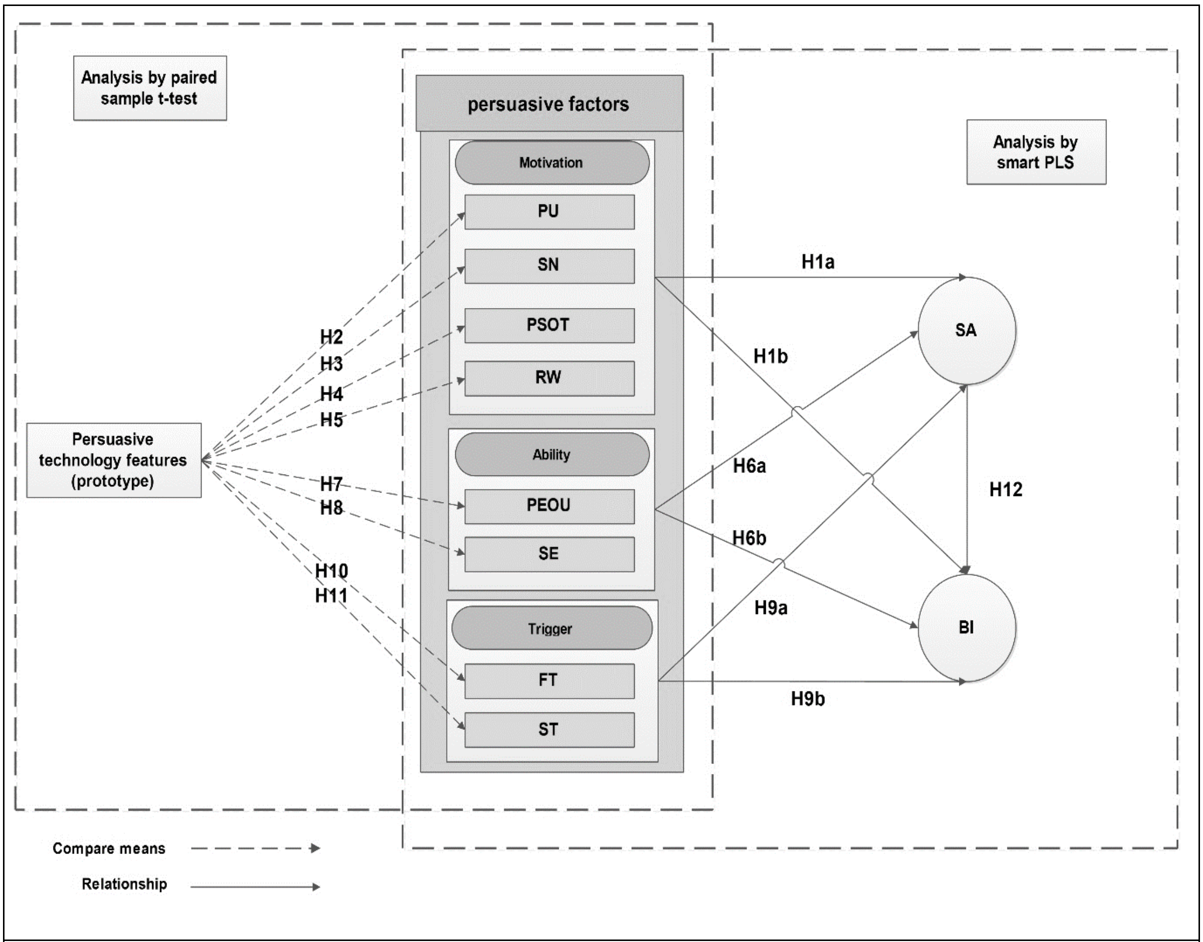
Fogg (2009) presented a new model for understanding people's behaviour to suggest that people are affected by three factors: ability, trigger and motivation. This model is known as the Fogg Behaviour Model (FBM). The FBM affirms that a person should have (1) enough motivation to perform a target behaviour, (2) be able to conduct the behaviour and (3) be triggered to perform the behaviour. These factors must take place at the same time; otherwise, the behaviour will not occur. FBM is useful for evaluating and implementing persuasive technologies to change people behaviour. In particular, persuasive technology pertains to how behavioural changes can be automated. It is possible to apply captology to a variety of fields, including health, the environment, personal relations, education, and community participation. Empirical studies have shown that persuasive technology can alter people's attitudes and behaviour to a certain degree (Fogg & Nass, 1997; Lenert et al., 2003). This study applies the application of persuasive technology to the awareness of information security.

In short, based on theories of information security awareness and behaviour and persuasive technology approach, the study applies FBM with security awareness' factors to investigate the effectiveness of persuasive technology to influence end-users' security awareness and intention to comply with ISPs.

3. FACTORS IDENTIFICATION AND HYPOTHESES FORMULATION

This research aims to explore the factors that influence information security awareness and compliance with ISPs, as well as build a model based on persuasive technology to incorporate these factors to improve end-users' security awareness and behavioural intention. In order to implement these security awareness factors in persuasive technology, the prototype has been developed to implement all factors based on persuasive technology strategies that are equivalent to these factors' operational definition. In that case, prototype features of persuasive technology strategies have been implemented in the prototype to represent the security awareness factors (refer to section 5).

The research model used in this study was built on an extensive literature review of previous studies to develop a persuasive security behaviour theoretical model. The model was improved based on the works on FBM (B. Fogg, 2009), TAM (Davis, 1989), TPB (Ajzen, 1991) and PMT (Maddux & Rogers, 1983; Rogers, 1975). As highlighted by Lebek, Uffen, Neumann, Hohler and Breitner (2014b), previous theories were confirmed to have a substantial influence on end-user security awareness and behaviour. The proposed model covers three kinds of dimensions, namely, motivation factors, ability factors, and trigger factors (see Fig. 1). In the following sub-sections, factors of FBM (motivation, ability, and trigger) along with the factors of security awareness are demonstrated.



Key: SA=Security Awareness, BI=Behaviour Intention, FT=Facilitator Trigger, PEOU= Perceived Ease of Use, PSOT=Perceived Severity of Threat, PU=Perceived Usefulness, SE=Self-Efficacy, SN=Subjective Norms and ST=Spark Trigger, RW=Reward

Fig. 1. Research Model

3.1. Motivation Factors

The first factor is a motivation factor based on FBM and indicates an individual's encouragement and desire to perform the particular behaviour in a given manner (Fogg, 2009). In persuasive technology design, the element of motivation should be sufficient to encourage the person to perform the action. Regardless of how detailed and successful an information security policy is in theory, it is not enough without end-users who are well aware of the security of information and motivated to follow established policy (Vance et al., 2012). Motivation is the key to successful information security awareness. Security awareness programmes are a popular way to improve information security attitudes and performance. However, ineffective security awareness could be a result of ignoring the motivation, which is fundamental to making security awareness effective (Parker, 2002).

Hence, people with high motivation are more likely to increase security awareness and perform security practices. Motivation is an essential factor in persuasive technology design to change end-user behaviour. The motivation in an information security context has an important effect towards increased end-user security awareness and intention to cooperate with ISPs. Accordingly, the present study hypothesised the following:

H1a: Motivation factors are positively related to security awareness of using persuasive technology.

H1b: Motivation factors are positively related to the security behaviour intention of using persuasive technology.

The motivation factors incorporated into the proposed model are perceived usefulness (PU), subjective norm (SN), perceived severity of threats (PSOT) and reward (RW).

3.1.1. Perceived usefulness

Perceived usefulness (PU) is intended to directly affect end-user motivation, in which the user is persuaded that the use of the particular technology is likely to boost work efficiency (Dinev & Hu, 2007). Ong and Lai (2006) reported that PU affects people's interest in technological acceptance because of the incentive value of outcomes. Users who believe in a positive relationship between use and results can build technology acceptance and influence behavioural intent to use this technology. (Davis, 1989).

PU in information security also explains the degree to which the end-user believes compliance with ISPs will strengthen the information security system and data protection (Xue & Liang, 2011). The PU requires that an end-user considers it is desirable and effective to comply with the information security guidelines. In addition, the intention of end-users to comply with ISPs' requirements is related to the extent to which end-users feel that the ISP's roles and responsibilities in the protection of information technology resources can improve their job performance (Al-Omari et al., 2012b; Siponen, 2000a). In the context of security awareness, TAM defines the intention of end-users to comply with ISPs, which is dependent upon the PU of information security measures (Lebek et al., 2014a).

In particular, persuasive technology can be used to implement PU to persuade end-users to increase security awareness and compliance with ISPs. Users who believe that compliance with ISPs has a positive effect in improving the information security system and protecting data assets will improve security awareness and the intent of ISPs to perform. As a consequence, when end-users believe the ISPs are valuable, they are more likely to influence and increase the motivation and actions to perform ISPs that enhance information security systems and job performance. PU was found to have a significant effect on security awareness and compliance with ISPs (Haeussinger, 2015a, 2015b; Lebek et al., 2014a). The present study, therefore, hypothesized the following:

H2: The perceived usefulness (PU) feature in the prototype has a persuasive effect of influencing end-users' security awareness.

3.1.2. Subjective norm

Subjective norm (SN) involves the social pressure to perform or not to perform the behaviour (Ajzen, 1991). Moreover, SN is also supposed to have an immediate effect on the compliance use of the system. The explanation is that people may choose to perform a behaviour even if they are not favourable to themselves in terms of behaviour or its results if they believe one or more important references and are motivated to meet the reference points (Venkatesh & Davis, 2000). Moreover, subjective norms rely on normative beliefs and the motivation to comply, based mainly on the perception that an important individual requires the person to conduct the relevant behaviour (Herath & Rao, 2009a).

In the context of information security, the subjective norm indicates how perceived external social factors affect end-users' compliance with the ISPs. According to Bulgurcu et al. (2010), a subjective norm is external social pressure on end-users regarding compliance with the ISP requirements because of the behavioural anticipation of these important referrals, such as professionals, friends and supervisors. In addition, previous studies show that subjective norms (normative beliefs) have a significant effect on the compliance of ISPs by end-users (Al-Omari et al., 2012b; Bulgurcu et al., 2010; Topa & Karyda, 2015). However, from the perspective of compliance with information security, SN depends on an overall assessment of end-user's intention to carry out ISP, as well as on normative beliefs towards compliance-related behaviour. The more feeling of pleasure that these behaviours are effectively controlled, the greater the intent to comply with ISPs (Lebek, Uffen, Breitner, Neumann, & Hohler, 2013). Particularly, to persuade end-users to increase awareness and compliance with the ISPs, the subjective norm will be implemented in persuasive technology design. Hence, this study hypothesizes the following:

H3: The subjective norm (SN) feature in the prototype has a persuasive effect of influencing end-users' security awareness.

3.1.3. Perceived severity of threats

The perceived severity of threats (PSOT) was initially adopted from PMT to clarify appeals for fear. PSOT assesses how serious people believe that threat will affect their lives (Milne, Sheeran, & Orbell, 2000). However, threat appraisal links with the awareness of how a person is endangered by an evaluation of the elements of fear appeal (Herath & Rao, 2009b). Furthermore, the threat shows the probability and seriousness of danger. It is usually the opportunity to lose something worthwhile. The value may include financial wealth, social status, health, emotional and business information or private information (Safa et al., 2015).

However, the perceived severity of threats (threat appraisal) concerns the assessment by end-users of the degree of risk resulting from careless conduct on information security. This threat will compromise the confidentiality, availability, and integrity of information. In addition, the threat appraisal was recognized as an important aspect that influences and affects people's perception and actions concerning ISP compliance (Bulgurcu et al., 2010; Lee & Larsen, 2009; Safa et al., 2015; Siponen, Adam Mahmood, & Pahnila, 2014). If end-users believe the threat is serious and concerned, they will very likely have a better perception of data protection, such as ISP performance. Moreover, end-users' perception of the severity of the threat significantly affects their security violations concern (Herath & Rao, 2009b). The perceived severity of the threats in persuasive technology design will be implemented to persuade end-users to increase awareness and comply with the ISPs. Thus, the following hypothesis is formulated:

H4: The perceived severity of threats (PSOT) feature in the prototype has a persuasive effect of influencing end-users' security awareness.

3.1.4. Rewards

An RW is one of the PMT variables that encourages individuals to react to dangerous behaviours or threats alerts. The RW is psychological or physical pleasure or recognition by peers, which increase the likelihood of maladaptive response. The rewards or benefits refer to any extrinsic or intrinsic motivation. Therefore, extrinsic and intrinsic rewards increase the chance of maladaptive response while awareness of vulnerability and threats will reduce the likelihood of such a reaction (Vance et al., 2012). The behaviour of people is conditioned by intrinsic and external motivation (Khair, Ahmad, & Hamid, 2017). It is essential to determine the factors that can motivate people to achieve high performance. Therefore, rewards are usually related to individual performance in a positive way (Siponen, 2000b).

In the field of information security, rewards are intangible or tangible benefits in exchange for the compliance of the ISP requirements given by an organization to an employee. They could include pay increases, monetary and non-monetary rewards, personal mention, promotions and recognition in written or oral assessment reports (Bulgurcu et al., 2010). However, the positive effects on high-interest tasks are achieved when end-users are verbally praised and tangible rewards are provided, which influence the end-user to adhere to security policies and procedures (Siponen et al., 2014).

In a persuasive application, the RW can be applied, and is an important strategy that has been found to motivate target behaviour. The reward has a positive influence on the persuasive application of technology, the more persuasive users are rewarded as a persuasive strategy they will be inspired to conduct a target behaviour and encourage behaviour change (Forget, Chiasson, & Biddle, 2008; Oyibo & Vassileva, 2011). It is therefore hypothesised that:

H5: The reward (RW) feature in the prototype has a persuasive effect of influencing end-users' security awareness.

3.2. Ability factor

The second factor of FBM is the ability to do something and increase the possibility of performing actions, which simplifies our behaviour (simplicity) (Fogg, 2009). Increasing the ability usually makes the behaviour simpler and easier to accomplish. Simplicity is a key factor in persuading people. Furthermore, human beings have a natural need to conserve resources, which means they are slothful. For instance, when a process involves easy work, such as pressing buttons on a computer or other tools many times, humans are more likely to continue immediately. However, if the processes are complicated and many steps are needed, people will most likely stay away or delay the process (Fogg, 2008).

According to Giraldo (Giraldo, 2014), the ability to perform the processes of security rules and procedures has a significant effect to increase end-users security awareness. In particular, the individual's understanding of how the action is carried out has been shown to have a major effect on the ability of a person to perform tasks, including the use of ISPs. It showed that people with higher ISP compliance abilities are more likely to use those systems in their work than people with fewer abilities (Ifinedo, 2014). Therefore, the following hypotheses are formulated:

H6a: Ability factors are positively related to security awareness of using persuasive technology.

H6b: Ability factors are positively related to the security behaviour intention of using persuasive technology.

The ability factors incorporated into the proposed model are perceived ease of use and self-efficacy.

3.2.1. Perceived Ease of Use

Perceived ease of use (PEOU) is described as what the end-user considers the action to be effortless and the ability to conduct actions to be understood. Therefore, PEOU is the perception of the amount of effort required to complete a particular task. (Davis, 1989; Dinev & Hu, 2007). Ease of use represents the personal issue or compliance facility. Amin (2009) claimed that PEOU has a substantial effect on behavioural and success intentions. It has been identified that PEOU has a significant effect on end-users' intention to accept the behaviour (Ong & Lai, 2006).

From the view of information security, the PEOU is connected to the degree to which an end-user feels that the use of relevant roles and responsibilities of ISPs is relatively simple and effort-free (Al-Omari et al., 2012b). End-users should improve their PEOU of the related information security measures and make their effectiveness as clear as possible (Haeussinger, 2015b). Concerning security awareness, the TAM indicates the intention of end-users to comply with ISP, which is influenced by PEOU in information security measures (Lebek et al., 2014a). The Security Acceptance Model (SAM) powered by the TAM significantly improves end-user information security awareness with ISPs compliance by increasing their perception that ISPs practice and engaging in the related roles and responsibilities as relatively simple (Al-Omari et al., 2012b). Dinev, Goo, Hu, & Nam (2006) pointed out that PEOU has a major role to play in influencing end-user compliance with ISPs. With the PEOU's positive effect on security awareness and compliance with ISPs, PEOU will use persuasive technology to encourage end-users to increase awareness and behaviour of the simplicity and effort-free use of ISPs. The following hypothesis is therefore formulated:

H7: The perceived ease of use (PEOU) feature in the prototype has a persuasive effect of influencing end-users' security awareness.

3.2.2. Self-efficacy

Self-efficacy (SE) is introduced in PMT and demonstrates a person's perception of his ability to achieve objectives. Bandura (1982) defines it as an individual's thinking of how to effectively conduct the behaviours required to deal with potential situations. Furthermore, persons with high self-efficacy will put in enough effort to succeed if done correctly, but people with low SE will most likely give up early and fail (Stajkovic & Luthans, 1998). Therefore, SE requires perseverance and dedication to overcome challenges that interfere with the use of these natural abilities to achieve objectives.

Bulgurcu et al. (2010) describe self-efficacy as an end-user's assessment of individual knowledge, abilities or competencies to meet the ISPs requirements. Self-efficacy is also the degree that the end-user feels the correct protective actions can be carried out (Vance et al., 2012). In addition, self-efficiency has an important effect on the intention of end-users to cooperate with ISPs. Companies produce productive training and security awareness programmes that ensure the ISA of end-users along with their SE follow ISPs (Bulgurcu et al., 2010). According to Safa et al. (2015), the belief that data and systems can be protected against unauthorized disclosure, alteration, failure, destruction and lack of availability relates to SE in the field of information security. Hence, SE in information security is recognised as a serious element that leads to security awareness and behaviour. SE in information security is therefore recognized as a major element contributing to security awareness and behaviour. SE is the most powerful indicator of intent to fulfil a behaviour. Therefore, self-efficiency in the security of information is the belief of end-users that they can implement and comply with information security procedures and policies (Siponen et al., 2014).

Furthermore, the role of SE in security awareness and behaviour has been evaluated through meta-analysis and determined that self-efficacy is highly correlated in ISP compliance (Herath & Rao, 2009b). The following hypothesis is formulated:

H8: The self-efficacy (SE) feature in the prototype has a persuasive effect of influencing end-users' security awareness.

3.3. Trigger factor

The third factor for FBM is trigger, which means that the action and target actions are performed immediately after the trigger feature is introduced. The concept of the trigger can be used in several names: call to action, cues, or prompts. A trigger is something that asks people to conduct the action now. If both motivation and ability are strong, actions can never take place without a proper trigger. This trigger can take different forms, including a text message, an alarm, an expressive image, a sales announcement etc. Nonetheless, the trigger must occur at the right time when people are highly motivated and capable of conducting the action (Fogg, 2009).

Implementing a new behavioural pattern involves a conscious decision and the new behaviour becomes increasingly automatic. Vance et al. (2012) believed that trigger is closely linked to usual behaviour, and then to the awareness of threats, trigger the cognitive process leading to intentional actions. Further, the usual behaviour is not merely through the behavioural sequence, but rather through the goals and means formed to achieve the objectives. The trigger in an information security context has an important effect towards increased end-user security awareness and intention to cooperate with ISPs. Hence, we hypothesize that:

H9a: Trigger factors are positively related to security awareness of using persuasive technology.

H9b: Trigger factors are positively related to the security behaviour intention of using persuasive technology.

In the sense of security of information, there are two types of triggers, the spark trigger and the facilitator trigger.

3.3.1. Facilitator Trigger

The second type of trigger is "facilitator" (FT). This kind of trigger is suitable for users with high motivation but are lacking in ability. The facilitator's goal is to trigger the behaviour and make the behaviour easier. Sparks, text, video, graphics and many more can be included as a facilitator. An effective facilitator informs users that the target behaviour is easy to do, that it will not require any resource at this time. For example, software updates often use facilitators to achieve compliance, which means a single click will accomplish the job. Most social networking sites have recently grown quickly by providing users with an "address book uploader," which only takes a few clicks to connect with lots of friends (Fogg, 2009).

Additionally, the facilitator helps motivated people who cannot complete the behaviour. The triggers facilitate the action or at least make the action appears to be easier (Yocco, 2016). The instructions given when setting up a new phone or computer are a typical example. Consequently, the facilitator trigger has been used in persuasive technology design to persuade end-users to influence security awareness and intention, which increases the ability to comply with ISPs. Therefore, this study hypothesizes the following:

H10: The facilitator trigger (FT) feature in the prototype has a persuasive effect of influencing end-users' security awareness.

3.3.2. Spark Trigger

Spark trigger (ST) is introduced in FBM (Fogg, 2009). A spark is a trigger that motivates behaviour. In the absence of an incentive to perform a target behaviour, a trigger with a motivating element should be designed, such a trigger type is called a "spark". Examples of sparks can vary from text to videos that inspire hope or highlight fear. In creating sparks for persuasive experiences, motivation elements can apply in the design for behaviour activation such as pleasure, pain, hope, fear, social acceptance, and rejection. Sparks can influence any of these elements of motivation. Sparks and other trigger styles can be viewed in various forms: the medium or the representation does not matter as long as the trigger is recognizable, connected to a target behaviour, and is delivered at a time when users can take action (Fogg, 2009).

Spark may be added to bring people hope or fear (e.g. exaggerated graphic images from current status). In addition, spark is a trigger added when there is low motivation but high ability. The trigger should be built together with an element of motivation (Chow, 2016). A spark boosts the motivation of an individual. Examples of spark triggers include advertising, ads and marketing messages; they want you to buy something that you are not inspired enough to purchase at present (Yocco, 2016). Accordingly, spark trigger has been implemented in the persuasive technology design to persuade end-users towards increasing the motivation in security awareness and intention of ISPs compliance. This study, therefore, hypothesizes that:

H11: The spark trigger (ST) feature in the prototype has a persuasive effect of influencing end-users' security awareness.

3.4. Influence of information security awareness on behaviour intention

ISA is mostly called a cognitive state of mind characterized by understanding the significance of information security and being mindful and aware of ISS goals, risks, threats, and have an interest in gaining the knowledge required to use IS appropriately (Siponen, 2000a). ISA is a critical factor in security behaviour that is structured as policy compliance with IS (Bulgurcu et al., 2010; D'Arcy, Hovav, & Galletta, 2009b).

However, it is usually suggested that ISA by itself is not adequate to describe ISP compliance and ISS behaviour (Haeussinger, 2015a). The result indicated by Dinev and Hu (2007) that end-users' awareness of issues and threats posed by unsafe technology is a strong precedent of their intention to use protective IS security technologies, such as anti-spyware. They also determine the positive effects on the intention of IS-users to use preventive technology of the three TPB constructs: attitude, subjective norm, and perceived behavioural control. Bulgurcu, Cavusoglu and Benbasat (2009) found that ISA and its perceived fairness have a positive effect on ISP's intention to comply. Empirically, Ryan (2006) has shown that higher user's ISA measures have a positive effect on user's information security practices in the workplace and at home. Yeo, Rahim, and Ren (2008) revealed that the web-based programme has a positive effect on three security aspects: email management, password management, and virus protection. They also show that persuasive technology features in web-based confirm the very strong effect in increasing end-users' information security aware behaviour. Therefore, the following hypothesis is proposed:

H12: Security awareness is positively related to the behavioural intention of using persuasive technology.

4. RESEARCH METHODOLOGY

The hypotheses in this study were tested in a laboratory experiment with a within-subjects design. A prototype was developed with persuasive technology strategies to investigate the effect on ISA and intention to comply with ISPs. In this study, we follow the seven-stage research approach based on quantitative and experimental methodology:

Stage 1: A literary review of awareness of information security, behaviour and persuasive technology was conducted. The literature review describes information security concerns and the most popular methods used to improve security awareness and behaviours of end-users such as TPB, PMT and TAM. In addition, how FBM, which explains how users can be made aware and change their behaviour, can be identified was conducted.

Stage 2: A model using mainly FBM with the three factors: motivation, ability, and trigger, was formulated. Under each factor, certain sub factors derived from most common theories (TPB, PMT and TAM), were identified and then, based on previous studies that applied these theories, the important factors that boost ISA and behavioural intentions of users were chosen.

Stage 3: A prototype that represents model factors by converting it to software features that adopt persuasive technology strategies was developed. The prototype aims to affect the ISA and behaviour of end-users. Using eight persuasive technology strategies: personalization, social learning, simulation, reduction, praise, tunnelling, suggestion, and rewards (Oinas-Kukkonen & Harjumaa, 2008a).

Stage 4: An experiment with students from International Islamic University Malaysia from different faculties and different levels of study (undergraduate and postgraduate). To ensure sufficient statistical power of 0.8 with a medium effect size of 0.3 for within-subject design, 100 subjects were recruited to participate in the final experiment who act as end-users (Cohen, 1988; Creswell, 2012). To begin, end-users completed the demographic and pre-prototype questionnaire before using the prototype. The questionnaire aims to gain insights into security awareness and behaviour. However, the strength of end-user security awareness was measured on a seven-point Likert scale from strongly disagree to strongly agree.

Stage 5: The prototype was used by end-users who had already completed a questionnaire that presumes to affect ISA and behaviour.

Stage 6: End-users carried out a post-prototype questionnaire to assess improved ISA and behavioural intention.

Stage 7: Paired-samples t-tests were conducted on the left side of the model (see Fig. 1), generally to validate the effectiveness of the prototype, and to compare the differences in the means between pre-prototype and post-prototype, and how persuasive technology strategies on PU, PSOT, SN, RW, SE, PEOS, ST and FT influencing end-users' information security awareness.

Stage 8: The PLS was implemented to test the proposed structural model on the right side of the model (see Fig. 1), to test the relationship between motivation, ability, and trigger factors with ISA and intention to comply with ISPs using persuasive technology (Yeo et al., 2008).

5. DESIGN OF PROTOTYPE

A prototype has been built in the form of an interactive interface that is based on several persuasive strategies to explore persuasive technology for information security. The prototype was developed to persuade end-users with information security best practices. Indeed, the persuasive strategies have been selected based on the factors integrated into the proposed model to improve security awareness, see Fig. 1. Hence, eight persuasive strategies from the collection of 28 described by Oinas-Kukkonen and Harjumaa were implemented in the prototype (Oinas-Kukkonen & Harjumaa, 2008a). The prototype covered, in particular, the following eight persuasive strategies:

- *Personalization:* A system that offers custom content or services is more persuasive.
- *Social learning:* An individual is encouraged more to conduct a target behaviour if he or she can use a system to observe others doing the behaviour.
- *Simulation:* Systems providing simulations will persuade them to observe the relation between cause and effect automatically.
- *Suggestion:* The system should recommend certain behaviours to users during the system operation process.
- *Rewards:* Systems that aim for rewards can have significant persuasive powers.
- *Reduction:* A system that reduces complicated behaviour to simple tasks helps users, achieve their target behaviour and improve a behaviour's benefit/cost ratio.
- *Tunnelling:* The use of the system to guide users through a process or experience offers the possibility to persuade them
- *Praise:* The system should use praise using words, pictures, symbols or sounds to give a user positive feedback

In IT literature, the four important aspects of information security have been selected: password management, phishing e-mail, public WIFI, and social media. Accordingly, these four main important security aspects were applied in the prototype with all persuasive technology strategies mentioned above to each security aspect. We labelled an operational system implementation of one persuasive strategy, a prototype feature. The prototype incorporated the eight persuasive strategies in the form of eight prototype features of eight persuasive factors. The prototype features followed the process model developed by Oinas-Kukkonen & Harjumaa (2008a) for the design of persuasive technologies. Table 1 shows the mapping between the persuasive factors, persuasive strategies and the prototype features.

Table 1: Mapping between persuasive factors, PT strategies and prototype features

No	Persuasive Factor	PT strategy	Prototype feature
1	Usefulness	Personalization	(Security customization), customize the provided information to the mentioned security issue to highlight the importance of performing security policy.
2	Subjective norm	Social learning	(Security statistical), Showing the real statistic and number of users who do not comply with related security policy.
3	Severity of threat	Simulation	(Adverse security story), Providing a real story on the damage severity by security policy non-compliance.
4	Reward	Reward	(Virtual security points), Points awarded for the correct answer to the security behaviour question.
5	Ease of use	Reduction	(Short security test), Providing a short test with multiple choices for answers to assess users' security compliance and easy prototype navigation.
6	Self-efficacy	Suggestion	(Security Recommendation), Providing recommended methods on how to properly perform security policy to avoid security threats.
7	Spark	Praise	(Security expression), Showing an expressive picture and sound related to the answer, which represents the user's situation with this security behaviour.
8	Facilitator	Tunnelling	(Simple security steps), Providing easy and simple steps to comply with the security policy.

6. DATA ANALYSIS AND RESULT

6.1 Subjects Background Information

Among the 100 participants, 64% were males and 36% were females. Participants' ages varied between 18 and 40 years. The majority of participants belong to small ranges, with 67.0% between 18–24 years of age, and 16.0% and 14.0% between 25–30 and 31–40 years, respectively. Further, 73% and 27% of the participants were undergraduates and postgraduates, respectively. According to participant nationalities, Malaysian participants represent over half at 60% and international participants represent 40%. However, majority of participants in information security activities are not aware of information security practices (74%) and only 26% of participants are aware of security practices.

6.2 Normality and Reliability

The assumption of normality was tested by the analysis of the variables' data distribution. To be effective in the paired sample t-test, the data must be normally distributed.(Pallant & Manual, 2013). The cut-off points for Skewness and Kurtosis set by Kline (2015) and Byrne (2013) between -2 to +2 and -7 to +7 respectively. Table2 presents a summary of the Skewness and Kurtosis of the variables used for this study that indicate the normality has not been violated. Thus, it can be concluded that the data set of all items were well-modelled by a normal distribution because the Skewness ranged between (-1.856 to -0.031) and Kurtosis between (-0.336 to 3.342). However, the values of Cronbach's Alpha were less than 0,7, which should be considered as poor and the value equal to or greater than 0,7 is appropriate to the reliability result and indicates a good level of internal consistency on a scale (Field, 2013). With a Cronbach alpha value of over 0.7 (range from 0.758 to 0.982), the result of the reliability test was achieved across all constructs in the questionnaire as shown in Table 2. Therefore, the questionnaire does not need to be revised and refined to increase the Alpha coefficients.

Table 2: Normality and Reliability Test Result

Factors	Mean		Normality				Reliability		
			Skewness		Kurtosis		Cronbach's Alpha		N of Item
	Pre	Post	Pre	Post	Pre	Post	Pre	Post	
PU	6.1917	6.6517	-1.150	-1.210	.583	.140	.905	.903	6
SN	5.5783	6.3003	-.592	-1.554	-.336	2.527	.834	.896	6
PSOT	5.8457	6.6186	-.908	-1.097	.306	.010	.878	.879	7
RW	4.9525	5.8693	-.736	-1.856	-.158	3.259	.961	.982	7
PEOU	5.7367	6.4383	-.549	-.905	.165	.012	.758	.862	6
SE	5.2293	6.2338	-.031	-.754	-.330	.050	.853	.883	7
ST	5.9967	6.6300	-.689	-1.292	-.299	.559	.931	.909	6
FT	6.0917	6.6567	-.967	-1.460	.257	1.403	.939	.906	6
SA	5.6922	6.5464	-.733	-1.045	.063	.204	.932	.929	9
BI	6.0667	6.5650	-1.177	-1.047	1.427	.204	.919	.908	6

6.3 Paired sample t-test results: the effects of the prototype

In the left side of the model, the paired samples t-test computes the mean difference of the values. It relies on the mean, variance, and number of data of the differences (Rietveld & van Hout, 2017). The purpose of this study was to evaluate the effectiveness of persuasive factors in the prototype for influencing participants' security awareness. Thus, a paired-samples t-test was conducted to determine whether a difference in the participants' mean scores of persuasive factors before and after they utilised the prototype can be observed and to determine whether the prototype used in this study was an effective conditional instrument for influencing ISA.

Table 3 shows the results of the paired sample t-test for all implemented persuasive factors in the prototype. The results indicate that after utilising the prototype, the participants' average mean scores increased significantly as evidenced by the p-value ($p < 0.001$) of all persuasive factors. The participants' mean score was significantly different before and after using the prototype as evidenced by the mean and standard deviations, respectively. The mean score and standard deviation after using the prototype were significantly higher than that before using the prototype. Consequently, the results of the paired-sample t-test confirmed the existence of a very strong persuasive effect for all persuasive factors applied in the prototype towards the participant's information security aware behaviour. Additionally, the prototype has a significant persuasive effect to influence participants' ISA and behaviour intention.

Table 3: Summary for paired sample test of persuasive factors

Persuasive Factors	N	Pre-prototype		Post-prototype		Paired Differences		t-value	DF	p-value Mean
		Mean	SD	Mean	SD	Mean	SD			
PU	100	6.1917	.83866	6.6517	.48496	.46000	.75065	**6.128**	99	**.000**
SN	100	5.5783	.98543	6.3003	.94277	.72167	1.44212	**5.004**	99	**.000**
PSOT	100	5.8457	.89725	6.6186	.53222	.77286	.85596	**9.029**	99	**.000**
RW	100	4.9525	1.6259	5.8693	1.44564	.91890	2.17296	**4.229**	99	**.000**
PEOU	100	5.7367	.78681	6.4383	.56041	.70167	.83863	**8.367**	99	**.000**
SE	100	5.2293	.88805	6.2338	.68007	1.00571	.87521	**11.491**	99	**.000**
ST	100	5.9967	.87584	6.6300	.52629	.63333	.78353	**8.083**	99	**.000**
FT	100	6.0917	.91972	6.6567	.47721	.56500	.82942	**6.812**	99	**.000**
SA	100	5.6922	.95801	6.5464	.55436	.85333	1.14198	**7.472**	99	**.000**
BI	100	6.0667	.88382	6.5650	.51187	.49833	.81011	**6.151**	99	**.000**

In addition, there is a significant difference in the mean score of persuasive factors (PU, SN, PSOT, RW, PEOU, SE, ST, and FT) for post-prototype and pre-prototype conditions, $p < 0.001$. The results in Table 3 indicate that the post-prototype mean score was higher than the pre-prototype mean score. In particular, our results suggest that the participants' security awareness increased when persuasive factors are applied in the prototype. Therefore, the hypotheses presented in this study were tested, the results show (see Table 3) that all hypothesized persuasive effects of all persuasive factors on influencing the end-users' security awareness are supported (H2, H3, H4, H5, H7, H8, H10, and H11 ($P < 0.001$)).

The findings indicate that Self-Efficacy (SE) had the highest value of differences among all persuasive factors by SE; t (99) = 11.491. While Perceived Severity of Threat (PSOT) and Perceived Ease of Use (PEOU) represented the second and third highest value of differences by PSOT; t (99) = 9.029, and PEOU; t (99) = 8.367, respectively. Meanwhile, Reward (RW) had the lowest value of difference among all persuasive factors by RW; t (99) = 4.229. Therefore, the Self-Efficacy (SE), Perceived Severity of Threat (PSOT), and Perceived Ease of Use (PEOU) persuasive factors play a significant role in persuading end-users to improve their security awareness in the context of using persuasive technology.

6.4 Modelling User Security Awareness in Persuasive Technology

Smart PLS (version 3.2.9) was used for the validation of the proposed research model on the right side of Fig. 1. PLS was used for two reasons: first, helps conduct high-quality theory-testing, second, is less sensitive to sample size issues, supports exploratory research (Fornell & Larcker, 1981). The analysis of this study includes the procedures for the after intervention (prototype) questionnaire, post-prototype distribution. In particular, PLS is performed to evaluate the psychometric properties of the measurement model, and the hypotheses were tested using the structural model.

6.4.1 Assessment of the Measurement Model

The estimation of the measurement model aims to assess the reliability and validity of the study's construct. The measuring model must ensure that its validity and reliability are adequate before checking the significant relationship in the structural model. Therefore, following the recommendation of Hair Jr, Hult, Ringle and Sarstedt (2017), in the context of the present study, the measurement quality of constructs was assessed by examining the convergent validity, individual item reliability, composite reliability, and discriminant validity of the measurement model. Because all of the constructs' measures had satisfactory reliability and validity assessments, all of the constructs' measurement items were maintained for testing the structural model. Then, we used structural model theory to validate the hypotheses.

First, we assessed the reliability and convergent validity of individual items in each construct by examining the factor loadings of individual measures on their underlying constructs, as well as the average variance extracted (AVE). The loadings of all measurement items on their respective constructs were more than the suggested minimum of 0.4. (Stevens, 2012), (see appendix A). All reflective constructs had AVE values greater than the minimum recommended value of 0.50 (Hair, Hult, Ringle, & Sarstedt, 2014), (see Table 4), showing that the items met the convergent validity requirement. Composite reliability (CR) and Cronbach's alpha were calculated to establish the scale's reliability and internal consistency. A scale is considered reliable if its CR and Cronbach's alpha is more than 0.70 (Hair et al., 2014). As shown in Table 4, all composite reliability values exceed 0.886 and Cronbach's alpha values exceed 0.846, demonstrating that all constructs that had the reflective scales were reliable.

Second, discriminant validity was established by examining the loading and cross-loading matrices (Appendix A), and the correlation matrix (Table 4). Each measurement item was significantly more loaded on its construct than on any other construct. Table 4 further reveals that each construct's square root of AVE is greater than the correlations between that construct and any other construct (inter-correlations) (Fornell & Larcker, 1981). As shown in Table 4 and Appendix A, each of the model's constructs meets these criteria for discriminant validity. As a result, our measurement model demonstrates adequate reliability and validity required for further testing of our research hypothesis.

Table 4: Composite Reliability, AVE, and Latent Variable Correlations

Variable	CR	CA	AVE	PU	SN	PSOT	RW	PEOU	SE	ST	FT	SA	BI
PU	0.934	0.92	0.612	**0.803**									
SN	0.917	0.891	0.648	0.424	**0.754**								
PSOT	0.924	0.9	0.669	0.688	0.557	**0.753**							
RW	0.896	0.86	0.59	-0.004	0.373	0.205	**0.94**						
PEOU	0.9	0.868	0.566	0.458	0.548	0.618	0.255	**0.768**					
SE	0.915	0.889	0.645	0.384	0.441	0.564	0.41	0.609	**0.741**				
ST	0.981	0.978	0.883	0.674	0.427	0.739	0.141	0.596	0.508	**0.809**			
FT	0.895	0.864	0.55	0.626	0.497	0.735	0.144	0.572	0.49	0.679	**0.818**		
SA	0.886	0.846	0.568	0.668	0.47	0.766	0.106	0.526	0.575	0.677	0.701	**0.782**	
BI	0.919	0.894	0.654	0.745	0.423	0.734	0.071	0.52	0.503	0.7	0.706	0.774	**0.805**

6.4.2 Assessment of the Structure Model

After the successful completion of the measurement model validation, the structural model was estimated. Predictive capabilities and the relationships between the constructs on the right side of the research model, as shown in Fig. 1, are estimated in the structural model by assessing the path coefficient beta (β), which represents the hypnotised relationships. This process clarifies the strength of the correlations among the dimensions in the research model (Hair et al., 2014). The strong correlation between dependent and independent constructs is depicted by the closeness of the path coefficient to 1. Fig. 2 shows the results of the model estimation, path coefficients, path significance based on a two-tailed t-test, and the variance explained by the independent variables (R^2). Based on these results (Fig. 2) all hypotheses were supported (H1a, H1b, H6a, H6b, H9a, H9b, and H12) ($p < 0.05$ and $P < 0.01$). The structural model explained approximately 69 per cent of the variance for the behaviour intention to comply in the context of persuasive technology, where 62.8 per cent of the variance could be explained by security awareness of using persuasive technology environment. However, the goodness-of-fit of the model had a large effect at 0.6484, which is sufficient for global PLS model validity.

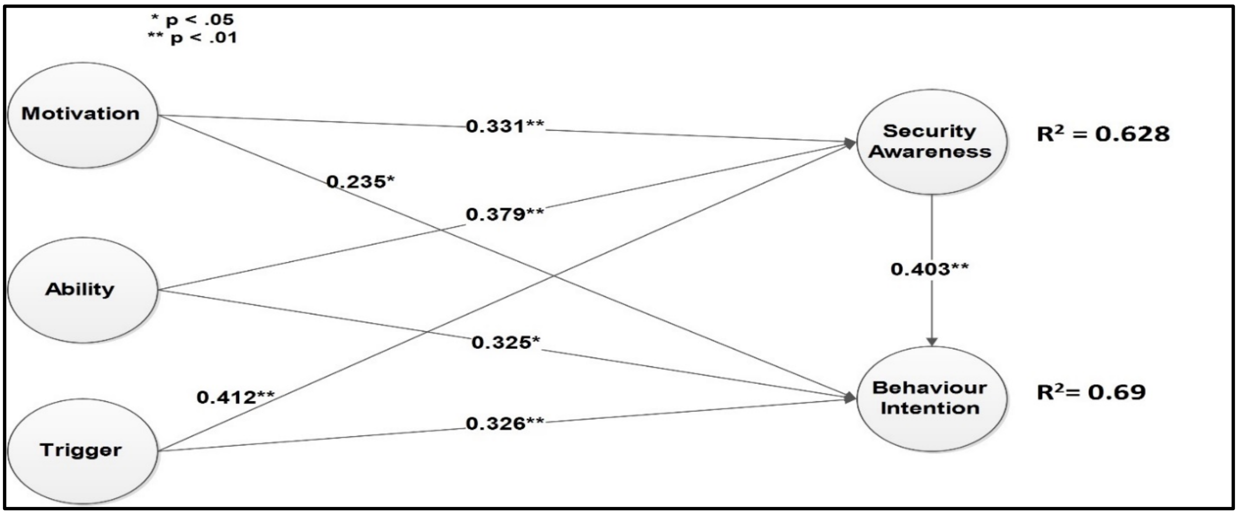


Fig. 2. Results of the Structural Model Testing

Based on the structural model results, the motivation, ability, and triggering factors have a strong and positive relationship with information security awareness and security behaviour intention in the context of using persuasive technology. In addition, information security awareness has a strong and positive relationship with security behaviour intention in the context of using persuasive technology. Therefore, it can be assumed that when the motivation, ability, and trigger factors in the persuasive technology context have a positive effect on the end-user, the end-user's security awareness and behaviour intention would positively increase.

7. DISCUSSION OF THE RESULTS

This study identified the factors that influence information security awareness in a persuasive technology context. The factors were identified based on persuasive technology design (FBM) representing three dimensions (motivation, ability, and trigger). The factors developed for influencing end-users' security awareness is based on common theories, such as PMT, TAM, and TPB. The theoretical model was developed for the factors influencing end-users' information security awareness in the context of persuasive technology use. In particular, it provides guidelines in creating a persuasive application that persuade end-users on the value of information security awareness improvement. In general, we found substantial support for our theoretical model and all hypotheses were supported by data gathered from 100 end-users.

In paired samples t-test, the results indicated that self-efficacy, perceived severity of threats, and perceived ease of use are the top persuasive factors influencing users' security awareness in the persuasive technology context. Self-efficacy (t-value=11.491) has a more persuasive effect than other factors, followed by perceived severity of threats (t-value= 9.029) and perceived ease of use (t-value=8.367). Furthermore, in smart PLS analysis, the findings indicated that ability, motivation, and trigger factors positively affect information security awareness of using persuasive technology. However, the ability factors (β = 0.379) had higher influence than the motivation and trigger factors. Therefore, ability (self-efficacy and perceived ease of use) factors are the most effective and persuasive in influencing information security awareness and behaviour intention. Additionally, promoting the ability through persuasive technology to utilise security rules and procedures processes has a significant effect on enhancing end-user awareness of security. In particular, understanding the way the action is carried out was shown to have a significant influence on a person’s abilities to perform tasks, including the use of ISPs. This finding is in line with studies that argued that security awareness is positively influenced by the ability of end-users to carry out security practices (Fogg, 2008; Giraldo, 2014; Ifinedo, 2014; Peltier, Peltier, & Blackley, 2005).

The results of this study indicated that the research model positively influenced the users towards improving information security awareness and behaviour intention in the environment of persuasive technology. Overall, the findings of this research indicated that facilitator trigger, perceived ease of use, perceived severity of the threat, perceived usefulness, self-efficacy, subjective norms, spark trigger, and reward influenced end-users’ security awareness in persuasive technology. In addition, ability, motivation, and trigger factors in the research model have a significant effect on awareness of information security and behaviour intention, which improved the security practices of the users. Therefore, persuasive technology, in general, has a positive effect on users’ security awareness and the intention of security behaviour. As a result, individuals, designers, and security managers in organizations should focus on these factors, which have a determining role in improving security awareness and increasing users’ efficiency in adopting the best security practices for the safe use of information technology.

8. CONCLUSION AND FUTURE WORK

This study provides a better understanding of how persuasive technology can be measured to improve ISA. The Fogg Behaviour Model was used as the underlying theoretical lens to examine information security awareness within the persuasive application. Moreover, the research investigated the most important factors that affect information security awareness and behaviour intention from the end-user’s perspective. Using the four theories (TPB, PMT, TAM, and FBM) offers a more comprehensive knowledge of ISA in the context of persuasive technology. This study developed and tested the research model empirically for ISA and behaviour intention within a persuasive technology context. The findings confirmed that motivation, ability, and trigger factors are positively related to information security awareness improvement, and consequently enhance behaviour intention towards best security practices. In addition, the prototype and its persuasive factors (PU, SN, PSOT, RW, PEOU, SE, ST, and FT) have a significant persuasive effect of influencing the end-users towards best security practices. This research makes a significant contribution to Human-Computer Interaction (HCI), specifically in the design and content of persuasive technology to influence and boost ISA and behaviour intention in the safe use of information technology. Moreover, creating programmes or applications using persuasive technology to persuade end-users to improve ISA and security practices can effectively help individuals and organisations to save time and money. Therefore, persuasive technology, in general, has a positive effect on users’ security awareness and the intention of security behaviour.

As with other empirical research, this study has certain limitations. First, this study was intended only from the viewpoint of one group of participants to examine the effect of persuasive technology. As a result, the findings of this study may not be generalized in different contexts. Thus, to further confirm and revalidate the results, future studies can include other groups, places, contexts, and usage times. Future studies should look at other viewpoints, for example, information system managers, chief information officers (CIOs), and information technology directors, to understand the features and relevant factors affecting these groups of people as stakeholders in ISS. Second, the long-term effectiveness of persuasive technology is still unknown. A longitudinal study on the use of persuasive technology is necessary to further understand how these findings are affected by usage experience and learning. Third, the research model of persuasive technology is not a fixed model and is subject to continuous evolution. Future studies may expand or amend this model by adding additional dimensions or factors appropriate for different security situations. Fourth, further development on the prototype requires more focus on the content, design, and persuasive features that can be implemented to persuade end-users in information security awareness. Finally, future research should investigate the effect of demographic data, such as age, gender, internet experience, and other moderating factors. Future studies should also investigate the effects of persuasive technology on younger, older, and end-users with disabilities.

REFERENCES

Abraham, S. (2011). Information security behavior: Factors and research directions. In *17th Americas Conference on Information Systems 2011, AMCIS 2011* (Vol. 5, pp. 4050–4062).

Ajzen, I. (1991). The theory of planned behavior. *Orgnizational Behavior and Human Decision Processes*, *50*, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012a). Information Security Policy Compliance : The Role of Information Security Awareness. In *Proceedings of the 18th Americas Conference on Information Systems (AMCIS '12)* (pp. 1–10).

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012b). Security Policy Compliance: User Acceptance Perspective. In *45th Hawaii International Conference on System Sciences* (pp. 3317–3326). IEEE. https://doi.org/10.1109/HICSS.2012.516

Amin, H. (2009). An analysis of online banking usage intentions: an extension of the technology acceptance model. *International Journal of Business and Society*, *10*(1), 27.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122.

Bawazir, M. A., Mahmud, M., & Molok, N. N. A. (2019). Persuasive Technology in The Islamic Perspective : The Principles and Strategies. *International Journal on Perceptive and Cognitive Computing (IJPCC)*, *5*(2), 107–116. https://doi.org/https://doi.org/10.31436/ijpcc.v5i2.88

Bawazir, M. A., Mahmud, M., Molok, N. N. A., & Ibrahim, J. (2016). Persuasive Technology for Improving Information Security Awareness and Behavior : Literature Review. In *International Conference on Information and Communication Technology for The Muslim World(ICT4M), 2016 6th International Conference* (pp. 228–232). IEEE. https://doi.org/10.1109/ICT4M.2016.49

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. In *Proceedings of the 15th Americas Conference on Information Systems (AMCIS)* (pp. 1–11). USA,California, San Francisco.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(2), 523–548. https://doi.org/10.1093/bja/aeq366

Busch, M., Patil, S., Regal, G., Hochleitner, C., Fröhlich, P., & Tscheligi, M. (2015).

Persuasive Information Security A Behavior Change Support System to Help Employees Protect Organizational Information Security. *Third International Workshop on Behavior Change Support Systems*.

Busch, M., Wolkerstorfer, P., Hochleitner, C., & Tscheligi, M. (2014). PAINLEsS – Personalized Multimodal Persuasive Ambient and Peripheral Interaction for Information Security. *Workshop on Peripheral Interaction: Shaping the Research and Design Space at CHI - Conference on Human Factors in Computing Systems*, 4.

Byrne, B. M. (2013). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. Psychology Press.

Chow, K. K. N. (2016). Lock up the lighter: experience prototyping of a lively reflective design for smoking habit control. In *International Conference on Persuasive Technology* (pp. 352–364). Springer.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (Second Edi). United States ofAmerica: Lawrence Erlbaum Associates.

Creswell, J. W. (2012). *Educational research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research* (4th ed). New Jersey: Pearson Merrill Prentice Hall.

D'Arcy, J., Hovav, A., & Galletta, D. (2009a). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

D'Arcy, J., Hovav, A., & Galletta, D. (2009b). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Davis, F. (1989). Perceived Usefulness, Perceived East of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.1016/S0305-0483(98)00028-0

Dhillon, G., & Backhouse, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM*, *43*(7), 125–128. https://doi.org/10.1145/341852.341877

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2006). User behavior toward preventive technologies – cultural differences between the United States and South Korea. In *European Conference on Information Systems (ECIS)*.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408. https://doi.org/10.17705/1jais.00133

Dolhalit, M. L., Abdul Salam, S. N., & Abdul Mutalib, A. (2015). Persuasive technology: A systematic review on the role of computers in awareness study. *Jurnal Teknologi*, *77*(29), 21–25. https://doi.org/10.11113/jt.v77.6806

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. sage.

Fogg, B. (1998). Persuasive Computers: Perspectives and Research Directions. *Chi 98*, (April). https://doi.org/10.1145/274644.274677

Fogg, B. (2002). *Persuasive Technology Using Computers to Change WhatWe Think andDo*. Ubiquity.

Fogg, B. (2008). Mass interpersonal persuasion: An early view of a new phenomenon. In *International Conference on Persuasive Technology* (pp. 23–34). Springer.

Fogg, B. (2009). A behavior model for persuasive design. *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive '09*, 1–7.

https://doi.org/10.1145/1541948.1541999

Fogg, B. J., & Nass, C. (1997). How users reciprocate to computers: an experiment that demonstrates behavior change. In *CHI'97 extended abstracts on Human factors in computing systems* (pp. 331–332).

Forget, A., Chiasson, S., & Biddle, R. (2008). Lessons from Brain Age on password memorability. *In Proceedings of the 2008 Conference on Future Play: Research, Play, Share*, 262–263. https://doi.org/10.1145/1496984.1497044

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*. https://doi.org/10.2307/3151312

Giraldo, G. (2014). Motivating Information Security Awareness (Isa): An Action Research Study. Proquest Llc. Syracuse University.

Haeussinger. (2015a). Information Security Awareness – A Review of the Literature: Definitions, Influence on Behavior, Antecedents. *Thirty Sixth International Conference on Information Systems (ICIS), Fort Worth*.

Haeussinger, F. J. (2015b). *Studies on Employees ' Information Security Awareness*. University of Göttingen.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Thousand Oaks*. *Sage*.

Hair Jr, J., Hult, G. T., Ringle, C., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. *Sage* (2nd ed.).

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. *The Journal of Strategic Information Systems*, *16*(2), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Khair, Z., Ahmad, N., & Hamid, M. azhar abd. (2017). Motivation in Islamic Perspective : A Review. *Research Gate*.

Kline, R. B. (2015). Principles and practice of structural equation modeling (methodology in the social sciences). New York, NY: The Guilford Press.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2978–2987. https://doi.org/10.1109/HICSS.2013.192

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014a). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014b). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

Lenert, L., Muñoz, R. F., Stoddard, J., Delucchi, K., Bansod, A., Skoczen, S., & Pérez-Stable, E. J. (2003). Design and pilot evaluation of an internet smoking cessation programme. *Journal of the American Medical Informatics Association*, *10*(1), 16–20.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health Related Behavior: A Meta Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Oinas-Kukkonen, H., & Harjumaa, M. (2008a). A systematic framework for designing and evaluating persuasive systems. In Springer (Ed.), *International conference on persuasive technology* (pp. 164–176). Berlin, Heidelberg: Springer.

Oinas-Kukkonen, H., & Harjumaa, M. (2008b). Towards deeper understanding of persuasion in software and information systems. *Proceedings of the 1st International Conference on Advances in Computer-Human Interaction, ACHI 2008*, 200–205. https://doi.org/10.1109/ACHI.2008.31

Ong, C. S., & Lai, J. Y. (2006). Gender differences in perceptions and relationships among dominants of e-learning acceptance. *Computers in Human Behavior*, *22*(5), 816–829. https://doi.org/10.1016/j.chb.2004.03.006

Oyibo, K., & Vassileva, J. (2011). Investigation of Social Predictors of Competitive Behavior in Persuasive Technology. In P. W. de Vries, H. Oinas-Kukkonen, L. Siemons, N. Beerlage-de Jong, & L. van Gemert-Pijnen (Eds.), *International Conference on Persuasive Technology*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-55134-0

Pallant, J., & Manual, S. S. (2013). A step by step guide to data analysis using IBM SPSS. *Australia: Allen & Unwin. Doi*, *10*, 1753–6405.

Parker, D. B. (2002). Motivating the Workforce to Support Security Objectives: A Long-Term View. *Fighting Computer Crime, A New Framework for Protecting Information*.

Peltier, T. R., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals*. Washington, D.C: CRC Press Company.

Preece, J. (2010). I Persuade, They Persuade, It Persuades! -technology-mediated social participation applications. In *Persuasive Technology Proceedings 5th International Conference PERSUASIVE 2010* (pp. 2–3). https://doi.org/ttp://dx.doi.org/10.1007/978-3-642-13226-1_2

Qudaih, H. A., Bawazir, M. A., Usman, S. H., & Ibrahim, J. (2014). Persuasive Technology Contributions Toward Enhance Information Security Awareness in an Organization. *International Journal of Computer Trends and Technology (IJCTT)*, *10*(4), 180–186.

Rietveld, T., & van Hout, R. (2017). The paired t test and beyond: Recommendations for testing the central tendencies of two paired samples in research on speech, language and hearing pathology. *Journal of Communication Disorders*, *69*, 44–57.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology: A*

Sourcebook, 153–176.

Ryan, J. E. (2006). A Comparison Of Information Security Trends Between Formal and Informal Environments. Auburn University.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, M. T. (2000a). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*, 31–41. https://doi.org/10.1108/09685220010371394

Siponen, M. T. (2000b). Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice. *Information Management & Computer Security*, *8*(5), 197–209. https://doi.org/10.1108/09685220010353178

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, *34*(3), 503-A5. https://doi.org/10.2337/dc10-0368

Stajkovic, A. D., & Luthans, F. (1998). Self-efficacy and work-related performance: A meta-analysis. *Psychological Bulletin*, *124*(2), 240.

Stevens, J. P. (2012). *Applied multivariate statistics for the social sciences*. Routledge.

Topa, I., & Karyda, M. (2015). Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 169–179). Springer.

Vance, A. (2010). Why Do Employees Violate Is Security Policies? Insights From Multiple Theoretical Perspectives. University Of Oulu.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204.

Wolmarans, A. (2003). Implementing an effective information security awareness programme. University of Johannesburg.

Xue, Y., & Liang, H. (2011). Punishment, Justice, and Compliance in Mandatory IT Settings. *Information Systems Research*, *22*(June 2011). https://doi.org/10.1287/isre.1090.0266

Yeo, A., Rahim, M., & Ren, Y. (2008). Use of Persuasive technology to change end user's IT security aware behavior: a pilot study. *World Academy of Science, Engineering and Technology*, *2*, 193–199. Retrieved from http://www.waset.org/publications/14957

Yocco, V. S. (2016). *Design for the mind: seven psychological principles of persuasive design*. Manning Publications Co.

Yu, T. (2012). Design of a persuasive recommendation agent to promote environmentally friendly products. University of British Columbia.

Appendix A

Item	Questions	Mean	SD	Loading
SA1	I am fully aware of threats, problems, and consequences of neglecting security practices.	6.470	.8463	0.685
SA2	I am fully aware of the potential cost of security problems such as weak passwords.	6.540	.7577	0.809
SA3	I am fully aware of how to effectively deal with security issues such as phishing emails.	6.440	.7696	0.821
SA4	I am fully aware of the advantages of following security practices.	6.590	.6977	0.817
SA5	I am fully aware that following security practices will keep my data safe.	6.580	.6694	0.742
SA6	I am persuaded to be fully aware of threats, problems, consequences of neglecting security practices.	6.570	.6073	0.799
SA7	I am persuaded to be fully aware of how to deal effectively with security issues	6.460	.6878	0.836
SA8	I am persuaded to be fully aware of the advantages of following security practices.	6.630	.6139	0.792
SA9	I am persuaded to be fully aware that following security practices will keep my data safe.	6.630	.5624	0.726
BI1	I intend to comply with the requirements of security practices such as creating very strong passwords.	6.570	.6397	0.775
BI2	I intend to protect my information resources by following security practices such as avoiding phishing emails.	6.570	.6553	0.788
BI3	I intend to comply with the security practices to protect my data.	6.570	.5904	0.74
BI4	I am persuaded to plan for complying with the requirements of the security practices.	6.530	.6269	0.824
BI5	I am persuaded to plan for protecting my information resources and following security practices.	6.580	.6225	0.845
BI6	I am persuaded to plan for complying with the security practices to protect my data.	6.570	.5730	0.851
FT1	Now, it is easy for me to create a very strong password if I am guided by simple and clear steps.	6.670	.5870	0.819
FT2	Now, it is easy for me to perform all protection methods to avoid phishing emails if I am guided by simple and clear steps.	6.600	.5860	0.872
FT3	Now, it is easy for me to comply with security practices to secure my data if I am guided by simple and clear steps.	6.670	.5870	0.849
FT4	Now, I am persuaded to create a very strong password if I am guided by simple and clear steps.	6.670	.5515	0.831
FT5	Now, I am persuaded to perform all protection methods to avoid phishing emails if I am guided by simple and clear steps.	6.640	.6117	0.74
FT6	Now, I am persuaded to comply with the security practices if I am guided by simple and clear steps.	6.690	.5449	0.79
PEOU1	It is easy for me to create a very strong password.	6.320	.8025	0.76
PEOU2	It is easy for me to avoid phishing emails.	6.370	.7870	0.719
PEOU3	It is easy for me to comply with security practices.	6.330	.7792	0.735
PEOU4	I am persuaded to create a very strong password if it is easy to create.	6.520	.6739	0.821
PEOU5	I am persuaded to avoid phishing emails if it is easy to avoid them.	6.540	.6730	0.762
PEOU6	I am persuaded to comply with the security practices if they are easy to comply with.	6.550	.6416	0.805
PSOT1	I believe that a weak password could be subjected to serious information security threats.	6.660	.6231	0.662
PSOT2	I believe that connecting to public Wi-Fi could be subjected to serious information security threats.	6.640	.7180	0.649
PSOT3	I believe that my data could be subjected to serious information security threats.	6.600	.7385	0.643
PSOT4	I believe that ignoring security practices could be subjected to serious information security threats.	6.630	.6139	0.793
PSOT5	I am persuaded to create a strong password if I believe that a weak password could be subjected to serious information security threats.	6.640	.6117	0.884
PSOT6	I am persuaded to not connect to public WI-FI if I believe that connecting to public Wi-Fi could be subjected to serious information security threats.	6.610	.7371	0.705
PSOT7	I am persuaded to follow security practices if I believe that ignoring security practices could be subjected to serious information security threats.	6.550	.8211	0.887
PU1	I believe that avoiding phishing emails is useful to protect my computer from malicious software.	6.650	.5198	0.791
PU2	I believe that creating a very strong password is useful to protect my personal information.	6.700	.5222	0.644
PU3	I believe that using security practices is useful to protect my data.	6.650	.6093	0.869
PU4	I am persuaded to avoid phishing emails if I understood the usefulness of avoiding phishing email.	6.620	.6159	0.889
PU5	I am persuaded to create a strong password if I understood the usefulness of the strong password.	6.670	.6204	0.793
PU6	I am persuaded to protect my data if I understood the usefulness of security practices.	6.620	.6479	0.811
RW1	I am willing to create a strong password if I get rewarded, e.g. gift, praise, certificate, etc.	5.890	1.5102	0.948
RW2	I am willing to avoid phishing emails if I get rewarded.	5.920	1.5021	0.93
RW3	It is important to me that my security practices are rewarded.	5.740	1.6120	0.867
RW4	Rewards motivate me to comply with security practices.	5.840	1.5224	0.949
RW5	I am persuaded to create a strong password if I get rewarded.	5.950	1.5201	0.966
RW6	I am persuaded to avoid phishing emails if I get rewarded.	5.880	1.4722	0.965
RW7	I am persuaded to comply with security practices if I get rewarded.	5.930	1.5259	0.95
SE1	I am very confident in my ability to create a very strong password.	6.350	.7571	0.697
SE2	I am very confident in my ability to protect my data when connecting to public WI-FI.	6.020	1.0729	0.695
SE3	I am very confident in my ability to perform my actions safely in social networks.	6.040	1.0142	0.719
SE4	I am very confident in my ability to comply with security practices.	6.190	.8726	0.763
SE5	I am persuaded to create a very strong password if I am very confident in my ability to create it.	6.410	.7398	0.759
SE6	I am persuaded to protect my data when connecting to public Wi-Fi if I am very confident in my ability to have a secure connection.	6.300	.8469	0.761
SE7	I am persuaded to comply with security practices if I am very confident in my ability to comply with them.	6.330	.8535	0.789
SN1	My friends think it is a good idea not to share personal information in social networks.	6.300	.9692	0.756
SN2	My friends think it is a good idea not to accept a friend request from strangers.	6.170	1.1286	0.568
SN3	Most people think I should follow security practices.	6.380	.9617	0.676
SN4	I am persuaded not to share personal information in social networks if my friends think it is a good idea.	6.340	1.3350	0.865
SN5	I am persuaded not to accept friend requests from strangers if my friends think it is a good idea.	6.250	1.3210	0.801
SN6	I am persuaded to follow security practices if most people think I should follow them.	6.360	1.2270	0.817
ST1	Now, I will be more motivated to create a very strong password if I see an expressive picture warning me of a weak password.	6.670	.5329	0.763
ST2	Now, I will be more motivated to create a very strong password if I hear an expressive sound warning me of a weak password.	6.630	.5801	0.762
ST3	Now, I will be more motivated to comply with the security practices if I see an expressive picture or hear an expressive sound.	6.620	.6479	0.806
ST4	Now, I am persuaded to create a very strong password if I see an expressive picture warning me of a weak password.	6.590	.7534	0.859
ST5	Now, I am persuaded to create a very strong password if I hear an expressive sound warning me of a weak password.	6.630	.6139	0.868
ST6	Now, I am persuaded to comply with security practices if I see an expressive picture or hear an expressive sound.	6.640	.6594	0.789