Abstract

Password manager applications have the potential to alleviate password pain and improve password strength, yet they are not widely adopted. Password managers are dissimilar to other kinds of software tools, given that the leakage of the credentials they store could give a hacker access to all the individual's online accounts. Moreover, adoption requires a deliberate switch away from an existing (manual) password management routine. As such, traditional technology adoption models are unlikely to model password manager adoption accurately. In this paper, we propose and explain how we validated a theoretical model of Smartphone password manager adoption. We commenced by carrying out exploratory interviews with 30 Smartphone owners to identify factors that influence adoption. These were used to develop a model that reflects the password manager adoption process, building on Migration Theory. The proposed model, MIGRANT (MIGRation pAssword maNager adopTion), was validated and subsequently refined in a week-long study with 198 Smartphone owners, combining self-report and observation to measure constructs. This study contributes to the information security behavioural literature by isolating the main factors that encourage or deter password manager adoption, and those that moor Smartphone owners in their current practices: hindering switching. With this investigation, we introduce migration theory as a reference theory for future studies in the information security behavioural field.

Keywords: Password Manager; Adoption; Migration Theory.

Introduction

Passwords are the first line of defence on any computer device or networked systems, constituting a crucial barrier between attackers and online accounts. Yet, people struggle to manage multiple strong passwords (Gallagher, 2019; Couillard, 2015), and engage in coping strategies such as using weak passwords (Bošnjak and Brumen, 2019), writing them down (Adams & Sasse, 1999; Hoonakker et al., 2009), or reusing the same password on multiple systems (Das et al., 2014). Smartphone password management is likely to be even more problematic, due to their multi-layer keyboards complicating typing and making it more time consuming. This encourages the use of even shorter and weaker passwords (Von Zezschwitz, et al., 2014). Predictable password behaviours make it easier for attackers to breach accounts (Das et al., 2014).

Password manager applications store all passwords securely (Silver et al., 2014), with access controlled by a master password. They eliminate the password memorial burden and make it easy for people to use a strong and unique password for each different site. Credential populating password managers help prevent shoulder surfing, brute force and dictionary attacks (Al-Sinani & Mitchell, 2010; Schechter, 2019). If they are configured to generate passwords, they also improve password strength (Friendman, 2014; Lyastani et al., 2017). Password managers thus reduce vulnerabilities by eliminating the need for people to engage in password memorial coping strategies.

Password managers have been endorsed by respected security professionals, such as Bruce Schneier (2014), and also by the UK's National Cyber Security Centre (2017). Despite this, and their obvious benefits, password managers have not yet been widely adopted (Hoonakker et al., 2009; Stobert and Biddle, 2014; Renaud & Zimmermann, 2019). Poor usability has been blamed for the paltry adoption (Seiler-Hwang et al., 2019) but the situation is likely to be more complex than a mere usability deficiency, as highlighted by these researchers (Pearman et al., 2019; Chaudhary et al., 2019; Ayyagari et al., 2019; Schechter, 2019). If we have a better understanding of exactly what deters or encourages password manager adoption, interventions can be specifically designed to improve adoption rates. The research reported in this paper was carried out to answer the following research question: "*Which Factors Influence Smartphone Password Manager Adoption?*".

We first review password manager related research and justify the use of Migration Theory (Lee, 1966) as our theoretical foundation. We then explain how we identified the constructs to be included in the model. We detail our proposed model and explain how we validated it using a longitudinal survey of Android Smartphone owners' migration to password manager adoption (as evidenced by the installation of any password manager). We report on our findings and analysis then discuss our findings and the limitations and conclude.

Background Literature

Before we discuss the related research, we need first to highlight the fact that password manager adoption is different from other kinds of Smartphone app adoption. There are two specific aspects influencing the password manager adoption decision, which will constrain our choice of a theoretical lens to ground our adoption model.

First, perceived risk: we have to acknowledge that password managers store account credentials — the keys to all online accounts. Loss of these could lead to financial and reputational harm (Koppel et al., 2016). This makes password managers subtly different from other apps, such as instant messaging tools, which do not store all the person's online credentials. The stakes are arguably much higher if a password manager leaks its stored information. Hence, potential adopters have understandable concerns and might be hesitant to trust these tools (Anderson, 2014; Maclean and Ophoff, 2018; Schechter, 2019).

Second, pre-existing practice: people already have their own password management routines, which will exert an influence over any decision related to changing these (Pearman et al., 2019; Renaud & Ophoff, 2019). Consider that children are given passwords when they start school, and accumulate more passwords as they age and start using more online services. Any modelling of password manager adoption must acknowledge the fact that such adoption replaces current password management routines and that this might be resisted as a consequence (Renaud et al., 2019; Johansson, 2016; Jost, 2015). Hence, we need a theory that incorporates a construct acknowledging the influence of existing routines on the adoption of new routines or tools that would change that routine.

Password Manager Research

A number of password managers are commercially available. Generally, there are three broad categories of software password manager:

- the *first* are built into browsers and let people save passwords that enter while using the browser. Examples of browsers offering this functionality are: Firefox, Google Chrome and Internet Explorer.
- the *second* can be installed as a browser extension. Examples are LastPass, DashLane and PwdHash.
- the *third* is the dedicated or stand-alone password manager. One example is RoboForm. (Many of these are also available as browser extensions.)

A number of hardware password managers also exist, including My Login Vault and myIDKey. Software password managers store passwords in different ways: (1) locally on the person's own device (such as KeePass), (2) cloud/web based (such as LastPass), and (3) those that do not store passwords, such as PwdHash, SuperGenPass, and Passpet.

A number of studies have been conducted to propose new, more secure, password manager applications (Ahuja et al., 2016; Wang et al., 2016; Li et al., 2017; Li & Evans, 2017;Patil et al., 2019; Wang & Sun, 2016), and analyse the security of existing password managers (Zhao et al., 2013; Gray et al., 2016). Some studies analyse the security of these applications theoretically, focusing on cloud-based password managers (Schougaard et al., 2016; Zhao et al., 2013; Li et al., 2014; Luevanos, 2017). Others have focused on password manager accessibility (Barbosa, 2016), their usability (Chen et al., 2018; Arias-Cabarcos et al., 2016; Chiasson et al., 2006; Karole et al., 2010; McCarney, 2013), or compare individuals' password manager preferences (Agholor et al., 2016).

Researchers have reported password manager adoption rates, with Table 1 providing a snapshot of these. This demonstrates that password manager usage has increased from 1% in 2007 (Tamil et al., 2007) to 10% in 2019 (Rogers, 1975), or as much as 19% in some studies (Wash et al., 2016). The only outlier is Stobert and Biddle's (2015) survey of security experts, reporting 40% adoption. The adoption rates are still relatively low, when compared to the adoption of other kinds of effort-saving tools (Hu et al., 2018) and the general trend of speedier technology adoption across the board (McGrath, 2013).

A recent study (Aurigemma et al., 2019) proposed a theoretical model of password manager adoption, which reflects the impact of a fear-based intervention on adoption, but does not incorporate pre-existing password practice as a construct. Renaud and Ophoff (2019) do acknowledge the possible influence of pre-existing password management practices, but their model has not been validated empirically.

Influential Adoption Factors

Researchers have carried out studies to identify specific factors that influence password manager adoption (Alkaldi & Renaud, 2016; Aurigemma et al., 2017; Fagan et al., 2017; McCarney, 2013; Johansson, 2016; Bicakci et al., 2011; Chaudhary et al., 2019; Chiasson et al., 2006; Maclean & Ophoff, 2018). Table 2 provides a summary of the factors they identified (Note that semantically-related factors are grouped under a single name).

Insert Table 1 About Here

Choosing a Foundational Modelling Theory

Information security studies that apply theoretical frameworks have been published in recent years and reveal a growing interest in understanding the factors that influence security behaviours. Here, we explain how we chose the theory to ground our model's foundation.

Theories used in Information Security

Lebek et al. (2014) carried out a theory-based review of information security related research, and provide a list of the theories that have been used in the information security domain. These include: the Theory of Reasoned Action (TRA) (Hale et al., 2002), the Theory of Planned Behaviour (TPB) (Ajzen, 1991), General Deterrence Theory (GDT) (Nagin & Pogarsky, 2001), Protection Motivation Theory (PMT) (Rogers, 1975), the Technology Acceptance Model (TAM) (Davis, 1985), Social Cognitive Theory (SCT) (Bandura, 2001), Constructivism (Fornell & Larcker, 1981) and Social Learning Theory (SLT) (Bandura & Walters, 1977).

We now consider each of these, in terms of the two constraints mentioned above. We can discount SLT and constructivism because, as Lebek et al. (2014) explain, these are essentially learning theories, and are unsuitable for modelling adoption. GDT, reflecting deterrence, is also not an adoption theory. TAM, TPB, TRA and SCT do not incorporate any notion of risk or vulnerability. PMT does not satisfy the second constraint. Hence, none of these popular models is a good fit for modelling password manager adoption.

Insert Table 2 About Here

Theories used in Modelling of Similar Technologies

Our next step is to identify theories that have been used to model adoption of other information technology tools. Anything to do with people's bank accounts could be argued to require trust and the majority of those who do switch to Internet-enabled banking, either via a web page or browser, have used a physical bank branch and cash before doing so. Hanafizadeh et al. (2014) carried out a systematic literature review of Internet banking adoption theories. They enumerate a number of theories that have been applied in this domain. TRA and TPB (mentioned above) appear, but have already been discounted. Three additional theories are mentioned: Social Cognitive Theory (SCT) (Bandura, 1986), Commitment-Trust Theory (CTT) (Morgan & Hunt, 1984) and Perceived Risk Theory (PRT) (Roselius, 1971). These, too, do not satisfy our constraints: SCT not satisfying the first, and CTT and PRT not satisfying the second.

Theories acknowledging the Influence of Pre-Existing Routines

What we needed, to model Password Manager adoption, was a theory that incorporated risk as well as a construct that acknowledged the existence and influence of existing practice i.e. one that models a switch from an existing to a new behaviour.

The crucial quality of migration theory is that it is not prescriptive about exact constructs to be used within the model, with this quality having facilitated its use across multiple disciplines (Brettell &. Hollifield, 2014). Hence, it can also be tailored to satisfy our first constraint. Migration theory also has, at its core, the notion of a geographical migration from an existing state to a new state (Lee, 1966). This satisfies our second constraint.

Migration theory has previously been used to model the adoption of other information technologies, such as cloud computing (Bhattacherjee & Park, 2014), instant messaging (Sun et al., 2017) and social networking services (Chang et al., 2014), but not has not yet been tested in the information security domain.

This theory assumes that migration decisions are the result of a calculus which incorporates negative factors in the current state, which encourage people to leave (also called 'push factors'), positive factors in the new state that attract people (also called 'pull factors'), and obstacle factors that constrain migration (also called 'mooring factors').

Having focused our attention on migration theory, we conducted a brief review of recent research into security behaviours in the broader field of information security. We discovered that the adoption predictors fall into three pertinent key categories (Ngoqo & Flowerday, 2015; Machuletz et al., 2016; Djeni & Erbilek, 2017; Vafaei-Zadeh et al., 2018):

First, the adoption or intention to adopt a secure behaviour, is affected by their perceptions of their current behaviours, such as the perceived severity or susceptibility to an online threat. These are similar to migration theory's push factors. (These align with constraint 2).

Second, behaviour, or behavioural intention, is affected by perceptions and expectations of the new behaviour, which can either positively influence the adoption (such as perceived response efficacy) or negatively deter it (such as response cost or privacy concerns). These are similar to migration theory's pull and mooring factors; respectively. (The mooring constructs align with constraint 1).

Third, individual differences, such as innovativeness, can predict adoption behaviours (Lu et al., 2005; Martínez-Román & Romero, 2017; Thakur et al., 2016). (Innovativeness is a person's propensity to adopt new technologies, as compared to others in their community.)

This kind of alignment with the features of migration theory confirms that it is worth exploring the application of migration theory to password manager adoption.

Research Model and Hypotheses

Insert Figure 1 About Here

The research stages are depicted in Figure 1.

Phase 1: To answer the research question posed in the introduction, we need firstly to identify the constructs to use in our model. Most technology adoption studies build their theoretical models using constructs that have been empirically verified in other studies. However, since password managers are different from other kinds of technologies, and because of the limited literature on password manager adoption, we conducted an exploratory study to investigate users' perceptions of password managers.

During Phase 2, we use the constructs that emerged from Phase 1 to construct the MIGRANT model of password manager adoption and propose nine different hypotheses to validate it.

During Phase 3, we carried out a longitudinal study to validate the model. Phase 4 analysed the data and Phase 5 provides and discusses the final validated MIGRANT model of Smartphone password manager adoption.

Phase 1: Identifying & Ranking Password Manager Adoption Factors

The authors we cite in Table 2 identified factors that either impede or encourage password manager adoption. Yet these factors are very different in character and influence. For example, F1 is a socially influencing factor, F3 is related to personal and past experience. F2, F4, F5 and F7 are related to the characteristics of the password manager, while F6 is related to a person's individual risk perceptions, which are also socially informed. The deterring factors are often the flip side of the encouraging factors. So, while F7 could be related to a person being convinced that the use of a password manager would help them to improve their general password security, the flip side of this factor could also be related to a person not being convinced of this, and citing concerns about how their

passwords are being stored, with this deterring adoption.

This list of factors, while being interesting and valuable, cannot be used to construct the MIGRANT model. Firstly, we do not have the frequency with which each factor was mentioned by interviewees (in the cases of surveys), which makes ranking difficult. Secondly, given that some of the data was collected online (Alkaldi & Renaud, 2016), it was hard to obtain more information about each participant's beliefs and justifications for their answers. Third, when using surveys, one can expect participants' opinions/perceptions to be framed by the posed questions. Finally, the factors emerged from studies in different contexts. This means that we cannot group these factors together as if they were all elicited in the same way. The dependencies between these factors are also unspecified at present. We thus carried out a series of semi-structured interviews specifically for the purposes of identifying factors to build the MIGRANT model.

It is appropriate for exploratory studies to gather new data as extensively as possible, in order to hear what end-users have to say, in depth. We used the factors in Table 2 as a guide to inform our semi-structured interview formulation, as recommended by Fishbein and Ajzen (2011). Using semi-structured interviews allowed us to explore salient beliefs and to arrive at a ranked list of factors influencing password manager adoption decisions. (see Appendix B for questions)

Semi-structured interviews were conducted with 30 Smartphone owners from April to June 2016, as advised by Fishbein and Ajzen (2011). The study was approved by the University of Glasgow's ethics review board. Sampling was convenience based with participants being recruited using social networking. Convenience sampling is often used in exploratory studies to obtain different views, to explore possible explanations or hypotheses, or to identify constructs (Ferber, 1977).

The sample included interviewees of different education levels, with an average age of 36.3 years. Of these, 18 were female (60%), and 12 male (40%). The majority of the interviewees were Android owners. Table 3 provides some examples of participant responses.

The transcripts of the interviews were analysed using thematic analysis, focusing on identifying themes and patterns related to password manager perceptions. First, three interviews were coded and then re-coded, independently, by a second coder. After that, a joint code book was created, which was used to code all the interviews. As each new concept was encountered, it was discussed with the second coder to agree on a new code before it was added to the code book.

Insert Table 3 About Here

The extracted factors fell naturally into the three categories that are related to individual choice, mirroring the categories reflected in migration theory, which confirms its potential in modelling the password manager adoption process. First, there are pull factors, which are related to the positive password manager features that could make a switch desirable. Pearman et al. (2019) mention convenience and faster logins as factors that could be considered to be pull factors. Then we have the push factors, related to perceptions of the person's current password management practice, as mentioned by Pearman et al. (2019) "Dissatisfaction with Current Method". Third, we have the mooring factors, which add friction to a change, as highlighted by Pearman et al. (2019) as "Satisfaction with Current Method". Finally, we have identified a number of cross-cutting factors. The full set of identified factors are listed in Table 4.

Insert Table 4 About Here

Phase 2: Proposing the MIGRANT Model & Hypotheses

Fishbein and Ajzen (2011) suggested that people's salient beliefs about a particular behaviour can be identified by checking the frequency of each theme in the collected qualitative responses, then selecting themes identified by at

least 20% of the interviewees (i.e., at least 6). Therefore, the qualifying factors will now be used to inform hypothesis formulation.

Pull Factors

Pull factors are password-manager-related factors that encourage migration. Two main pull factors emerged from the analysis of the interviews: (1) the usefulness of password managers, and (2) their effectiveness in improving the security of passwords and online accounts. This confirms previous research into the adoption of other security tools and measures. In particular, a study showed that perceived effectiveness of security policies had a positive influence on individuals' intention to comply with these policies (Hovav & Putri, 2016). Furthermore, according to the IT adoption literature, one of the strongest predictors of adopting new technology is the perception of how useful that adoption will be, i.e., 'perceived usefulness'. Instead of evaluating the perceived usefulness independently, in the case of technology migrations, usefulness is evaluated against the person's current password management practice before adopting the new technology. In the literature, this construct is called 'relative usefulness' (Bhattacherjee & Park, 2014). Two pull-related hypotheses are proposed:

Hypothesis 1 (H1): Perceived relative usefulness of password managers is positively related to the intention to adopt a Smartphone password manager.

Hypothesis 2 (H2): Perceived response efficacy of password managers is positively related to the intention to adopt a Smartphone password manager.

Push Factors

These are the factors that propel people towards the use of password managers. Prior research shows that a primary reason for people to adopt new technology is their dissatisfaction with their current product or service (Bhattacherjee & Park, 2014; Fan and Suh, 2014). (Dissatisfaction being the state of being unhappy about a service or product based on poor experience.) We aim to find out whether, if a person's evaluation of their current method for managing their passwords is unsatisfactory, they will be more likely to consider using a password manager. These are the factors that align with constraint 2.

Based on the analysis of the interviews, the main sources of dissatisfaction were: (1) the perceived cost of managing passwords, and (2) their perceived vulnerability. The following push-related hypotheses are proposed:

Hypothesis 3 (H3): A person's dissatisfaction with their current password coping method is positively related to their intention to adopt a Smartphone password manager.

Hypothesis 3.a (H3a): The perceived vulnerability related to a person's current password coping method is positively related to their dissatisfaction with their existing method.

Hypothesis 3.b (H3b): The perceived response cost related to managing passwords with their current password coping method is positively related to dissatisfaction with their existing method.

Mooring Factors

Despite the presence of pull and push factors related to password manager adoption, some other factors might add friction to migration. Previous migration-theory-based research found switching costs to negatively affect migration intention (Bhattacherjee & Park, 2014; Chang et al., 2014; Schreiner & Hess, 2015). Likewise, the results of the interviews revealed that the costs associated with password manager migration — such as set-up, learning and monetary costs — could discourage adoption. Furthermore, given the sensitivity of data stored by a password manager, and due to the perceived risks when using password managers, people might be reluctant to adopt them (the first adoption constraint).

As such, the perceived risks related to password managers is included as a mooring factor (Aurigemma et al., 2017). Security and privacy concerns over using password manager applications were found to be one of the main factors influencing the perceived risk of using the password manager (Alkaldi & Renaud, 2016). These are the factors that align with constraint 1. Therefore, the following mooring-related hypotheses are proposed:

Hypothesis 4 (H4): The perceived risk of using password managers is negatively related to the intention to adopt a Smartphone password manager.

Hypothesis 4.a (H4a): Security concerns over using a password manager tool are positively related to the perceived risk of using a Smartphone password manager.

Hypothesis 4.b (H4b): Privacy concerns over using a password manager are positively related to the perceived risk of using a Smartphone password manager.

Hypothesis 5 (H5): The perceived cost of learning how to use a password manager is negatively related to the intention to adopt a Smartphone password manager.

Hypothesis 6 (H6): The perceived cost of setting up a password manager is negatively related to the intention to adopt a Smartphone password manager.

Hypothesis 7 (H7): The perceived monetary cost of using a password manager is negatively related to the intention to adopt a Smartphone password manager.

Other Factors

Besides push, pull and mooring factors, there are also other factors that could impact switching decisions. Only one factor identified during the interviews was mentioned enough times to be included i.e., descriptive norms.

Descriptive Norms: these, also called "social influence" in the literature, are defined as "what individuals perceive others around them are commonly doing" (Cialdini et al., 1990). These have been found to be predictors of the intention to adopt security systems (Tu et al., 2014; Lee & Larson, 2009) such as anti-virus software (Lee & Larson, 2009). The analysis of the interviews also revealed that interviewees were reluctant to adopt password managers because they "did not want to be first" among their friends and family members to do so. Therefore, this factor has been included in the model.

Hypothesis 8 (H8): The descriptive norms of using a password manager are positively related to the intention to adopt a Smartphone password manager

Intention and Actual Adoption

As this research aims to study the factors that affect password manager adoption behaviour, the adoption construct was considered. While the intention to adopt a password manager reflects the likelihood of adoption, actual adoption behaviour commences when Smartphone owners install a password manager on their device. The extant human behaviour literature identifies behavioural intention as a main antecedent of actual behaviour (Fishbein & Ajzen, 2011), and it has been shown to be a significant predictor of actual behaviour (Kim et al., 2008; Vasileiadis, 2014). Due to difficulties in recording actual security behaviours, many information security studies stop short of measuring actual behaviours (Pham et al., 2017). Instead, they measure security intention and argue that it is a reasonable proxy for actual behaviour (Pham et al., 2017). A systematic review of information security policy compliance studies found that few studies investigated actual behaviours (Sommestad et al., 2014) and concluded that the best predictor of actual security behaviour is behavioural intention. Thus, the following hypothesis is proposed:

Hypothesis 9 (H9): The stated intention to adopt a Smartphone password manager is positively related to the actual adoption of a Smartphone password manager.

Control Variables

Control variables are not central to the model, but may nevertheless impact the dependent variable, i.e., adoption intention.

Intention Influences: The control variables for this study, those that might influence a user's intention to adopt a password manager, are: (1) innovativeness, (2) age, and (3) gender.

We included gender as a control variable because previous studies suggested that there are differences between males and females in terms of their attitudes towards their Smartphones. Skog (2002) has reported that while males emphasised the functional features of Smartphones, females paid more attention to their appearance. Barn et al. (2014) also found that male students were less cautious about their privacy than female students. Males were more willing to share their personal data, including contact details, with mobile applications and more likely to shop online using their Smartphones.

Age is also included as a control variable, because existing research noted that the younger generation prefers to use online banking (Köse, 2009; Maduku, 2013). It might be the case that young users would be more willing to use a password manager.

Furthermore, those with a higher level of innovativeness are often more willing to take risks, and consequently to accept and trial new technologies (Thakur et al., 2016; Frimpong et al., 2017). This might also impact willingness to adopt a password manager, and has been included in other technology-related adoption studies, for example (Slade et al., 2015; Alalwan et al., 2018; Acheampong et al., 2017; Oliveira et al., 2016). It is important to note that innovativeness is not included as a construct in the model, because it was not mentioned by at least 6 of our interviewees. We did include it as a control variable, however, because of the strong evidence in the literature related to its impact on all adoption decisions.

Dissatisfaction Influences: Two other control variables that may impact dissatisfaction with current password coping behaviours are: (1) experience of being hacked, and (2) the number of passwords that a person needs to manage. Because the cost of managing passwords depends on the number of passwords that users have to manage (Zhang-Kennedy et al., 2016), this variable was included as a control variable influencing dissatisfaction with current coping behaviours. Finally, experience of being hacked might play a role in terms of users' perceptions of being vulnerable to attack (Alkaldi & Renaud, 2016). Exposure to hacking was thus also included as a control variable influencing dissatisfaction, as a dependant variable.

Figure 2 depicts the model that we will validate in the next section.

Insert Figure 2 About Here

Phase 3: Methodology

We developed a mobile application named CyberPal as an Android application, to provide a means to support two different studies (Figure 3):

Study 1: Validating the MIGRANT model: CyberPal was used as a mobile-based platform for harnessing the survey, and to detect whether intention was converted to behaviour i.e., installation of a password manager.

Study 2: Testing Intervention Efficacy: CyberPal was also an intervention harness that recommended a password manager based on users' stated requirements. The recommender system essentially supported the user choice process. Consider that adopters have to choose the preferred features of the password manager. For example, they choose whether they want a cloud-based password manager or a password manager that store their passwords locally in their devices. Study 2 tested different ways of supporting the choice.

CyberPal administered the survey questions for Study 1 before the intervention was delivered. Then, it allowed participants to express their preferences and supported the choice of a password manager (Study 2). CyberPal continuously monitored applications on users' devices to detect installation of a password manager.

It is important to note that Study 1, described in this paper, used the survey data and the stated intention to install a password manager (before the intervention was administered) in order to validate the MIGRANT theory of adoption. The conversion of intention to adoption was calculated for all participants, regardless of Study 2 experimental condition.

Measurement

Construct measurement is based on instruments that have already been published and modified to align with the study's context (see Appendix A).

All questions collected responses using a seven-point Likert scale, with options ranging from 'strongly disagree' (1) to 'strongly agree' (7). Finally, the dependent variable actual behaviour was measured by periodically retrieving all the applications installed on the participants' Smartphones and checking whether or not they had installed a password manager.

The questionnaire was reviewed by two security and information management researchers, who confirmed its validity. Before initiating the large-scale survey, a pilot test of the questionnaire was conducted with 15 testers who were aware of the existence of password managers.

Insert Figure 3 About Here

Data Collection

An invitation to participate was sent to 219,221 Android owners, using the Facebook advertising service, between July and September 2017. Participants were asked to install the application, answer the questionnaire and keep the application on their devices for a week for the chance to win online vouchers up £50. 645 people responded to the invitation and participated in the study.

We wanted to focus on people who already knew what a password manager was, and what it was used for, so that we did not conflate awareness with adoption, which are two different constructs. Thus, at the beginning of the survey, participants were asked whether they were aware of password managers. To confirm their familiarity, participants were asked to select the names of two popular password managers from amongst five password manager names. The five names actually included only two password managers, the rest being names of screen-locking mobile applications. 232 participants said they were aware of password managers. After reviewing their responses, 12 were removed for not completing the survey, 7 for not answering the validation question correctly, one for not keeping the application on their device for the required full week and 14 for not engaging with the survey. After discarding these responses, 198 completed surveys and were retained for analysis. 64% of participants were male, 34% female. About 70% were under 35 years of age. The majority had been educated beyond high school level. Only 3 participants were already using a password manager (Table 5).

Insert Table 5 About Here

Phase 4: Results and Analysis

The data analysis proceeded in four stages. The first stage screened the data to ensure validity to support subsequent analysis; the second stage generated a descriptive analysis of the dataset; the third stage focused on assessing the validity of the constructs used in the model; and the last stage was directed at hypotheses testing and model analysis using structural equation modelling (SEM). Using SEM for data analysis has become popular recently in the information management literature. Generally, a SEM model is composed of two sub-models: (1) a measurement model and (2) a structural model (Kline, 2015). The measurement model defines the relationships between the observed and latent variables. The structural model, on the other hand, explains the relationships

between the latent variables in order to test whether a particular latent variable influences another latent variable in the proposed theoretical model (Hair et al., 2010; Kline, 2015). The data was analysed using SPSS 23 and AMOS 23 software.

Stage 1: Data Screening

Before commencing the analysis, the data were screened to evaluate their validity to determine if they met the assumptions of SEM. Therefore, several tests were conducted. First, the data were scanned for missing data. From the scanning process, 6 cases were identified with randomly distributed missing data. The Missing Completely at Random (MCAR) test confirmed that these missing values were indeed completely random ($p = .785$)[1]. The MCAR value indicated that missing values in the dataset were randomly missed ($p > .05$). These missing data were imputed using the median value technique, a commonly used technique that is applied to compensate for missing values in quantitative studies.

Second, descriptive analysis of the dependent and independent variables was conducted to ensure the data is normally distributed (Table 6). The table shows that the kurtosis values for all the variables are less than 2 and the skewness scores are all within the acceptable range, which suggests that the data are normally distributed[2].Third, the outliers were tested by evaluating the standardised Z scores of (± 3.29) in each variable (Tabachnick et al., 2013(p.107). The standardised Z values for the dataset were between valid ranges. Fourth, this process was followed by evaluating linearity and homoscedasticity, which are important assumptions for linear regression models (Hair et al., 2010)[3]. Linearity and homoscedasticity were evaluated by examining the scatter plots (Kline, 2015). The inspection of the scatter plots revealed an oval shaped array of points, suggesting that variables are linearly related and homogenously distributed.

Insert Table 6 About Here

Finally, to determine whether two or more constructs represent the same external reality, a multicollinearity test is required (Hair et al., 2010; Tabachnick et al., 2013)[4]. Table A.2 (in Appendix A) shows that inter-correlations between variables range from .06 to .83. Also, multicollinearity can be evaluated through the Variance Inflation Factor (VIF) (Kline 2015). If VIF>10 this is an indication that two variables are highly correlated and a multicollinearity problem is presented (Kline, 2015). The calculated VIF values ranged from 1.201 to 5.011 (Table 7), which did not exceed the recommended cut-off value of 10. Accordingly, this stage confirmed that the data set of size 198 was valid and usable for testing the hypotheses.

Insert Table 7 About Here

Stage 2: Descriptive Analysis

During this phase, a descriptive analysis of participants' demographic data was carried out. Table 5 shows the demographic profiles of the respondents and their password manager app usage.

Stage 3: Measurement Model

A measurement model represents the relationship between the variables and their measures (Hair et al., 2010). This stage aims to examine the model by assessing both: (1) the constructs' validity and reliability, and (2) the model-fit indices, which are used to estimate the measurement model. A confirmatory factor analysis (CFA) was conducted to achieve this aim. In the CFA model, items are grouped according to the component definition from which the items came. Then, the item groupings are combined to form composite scores. If the composites show satisfactory measurement properties, they can be used in the final structural model (Hair et al., 2010; Kline, 2015).

Construct validity and reliability

The CFA is conducted to evaluate the degree to which a set of indicators constructing a scale all measure one thing in common (Kline, 2015). This uni-dimensionality can be evaluated by testing both the convergent and discriminant validity of all the constructs in the model (Zhu, 2000).

Convergent validity is the extent to which the measures that are theoretically related are also correlated (Zhu, 2000). Evaluating convergent validity relies on three indicators: (1) the item reliability of each construct, (2) the Average Variance Extracted (AVE) for every construct, and (3) the reliability of each construct (Tabachnick et al., 2013; Fornell & Larcker, 1981).

First, the item reliability of each construct is assessed by examining the loading of each indicator, in the measurement model, on their constructs. Items should only be retained if they have a strong factor loading, which indicates that the construct is well defined by its items (Hair et al., 2010). It has been recommended to retain the items in the measurement model that have a factor loading exceeding 0.50 (Hair et al., 2010). The factor loading of each item was computed in the CFA analysis. As shown in Appendix A, the loading of all items is greater than the cut-off value of 0.50, indicating that all the items are strongly related to their relevant factors.

Another indicator for verifying convergent validity is the AVE of each construct. AVE is computed for each construct by adding all the squared values of the factor loading of its items and then dividing the sum by the number of items representing the construct (Hair et al., 2010). The value of AVE should be at least 0.5 for it to be acceptable, indicating that a factor explains more than 50% of the variance of its items (Hair et al., 2010). The AVE was calculated using the Stats Tools Package developed by Gaskin (2102) and the output of the CFA analysis. As shown in Table 8, the AVE values for all constructs are greater than the minimum accepted point, reflecting an adequate convergent validity.

Insert Table 8 About Here

Convergent validity can also be evaluated through construct reliability. Construct reliability is the degree to which a set of two or more indicators (items) share the measurement of that construct. It measures the internal consistency and homogeneity of the items that comprise each scale (Hair et al., 2010). A construct is highly reliable when all its items are highly correlated, indicating that they are measuring the same construct. Construct reliability was tested with Cronbach's Alpha. Table 9 shows the Cronbach's Alpha values for all variables. (A Cronbach's Alpha value of 0.70 or higher suggests good construct reliability (Hair et al., 2010)). All the reliability scores in the study ranged between .703 and .973, supporting the convergent validity of the measurement model.

Insert Table 9 About Here

Discriminant validity is the extent to which concepts that should not be related theoretically are not intercorrelated (Zhu, 2000). It can be verified when the correlation value shared between a construct and any other construct is less than the correlation value of the construct and its items (Hair et al., 2010). Therefore, if the square root of the AVE value of a construct is greater than any correlation between this construct and any other construct, then that construct is more correlated with its indicators than any other construct in the model. The correlation matrix for discriminant validity was generated by the Stats Tools Package using output from CFA analysis. As illustrated in Table A.4 (in Appendix A), the square root of AVE values, represented at the top of each column, is greater than any other correlation in that column. This indicated that all constructs in the model are different from each other, supporting the discriminant validity of the model scales.

Model Fit:

The next stage, in evaluating the measurement model, is to measure the model fit in order to determine the extent to which the indicators (items) operationalise the latent variables (constructs). The measurement model fit refers to

how well the proposed model of the factor structure reasons about the correlations between variables in the dataset (Hair et al., 2010; Hooper et al., 2008). If the model is able to account for all the main correlations in the model, then the model has a good fit. If not, then there is inconsistency between the proposed and the observed correlations in the data, and the model is low fitted. A low-fitted model requires changes and modifications to the original model to enhance the fit (Kline, 2015; Byrne, 2013). There are different statistics used to determine the goodness of model fit. Although there is no universal agreement upon number of statistics to report, a minimal set would include the chi-square value, an index to describe incremental fit, such as the TLI, and a residuals based measure (such as RMSEA or SRMR). Chi-square compares the observed covariance matrix with the theoretically proposed covariance matrix. It is the only exact test for SEM models to evaluate the model fit to data (Barn et al., 2014). However, researchers often report other fit indices to evaluate their models. Other commonly used measures are: the Incremental Fit Index (IFI), which compares the chi-square of the hypothesised model to the null model that assumes that all variables are uncorrelated, the Comparative Fit Index (CFI), which measures the relative improvement in the fit of the tested model over the proposed model, the Tucker-Lewis Index (TLI), which is based on the idea of comparing the proposed factor model to a model in which no interrelationships at all are assumed among any of the items, and the Root Mean Square Error of Approximation (RMSEA), which estimates the difference between the examined model and a hypothetical model where every component in the model is related to every other component (Hair et al., 2010; Tabachnick et al., 2013). Table 10 (left) provides the minimum accepted cut-off points for all these measures.

Insert Table 10 About Here

The measures for the model fit were computed through CFA analysis. The goodness of fit values for the measurement model are specified in Table 10 (Right). These values are all within the acceptable scale for a good fit specified in Table 10 (Left), indicating that the measurement model fits with the sample data.

Stage 4: Structural Model

The proposed hypotheses were tested through SEM using the model in Figure 2 as a base model. Different techniques are used to explain the structural model. The goodness of fit of the proposed relationships between the constructs to the data was assessed. Furthermore, as suggested by (Kline, 2015; Hair et al., 2010), the parameter estimates of the structural model were examined to understand the effect of the independent variables on the dependent variables, as suggested in the theoretical model.

As illustrated in Table 11, the normal Chi-square value was 1.557, indicating a good fit of the structural model. Also, the RMSEA value was .053, which implies adequate model fit. Furthermore, IFI= .990, TLI= .948, CFI= .989 suggesting a reasonable fit of the model to the data. To sum up, the evaluated values of the fit indices indicated that the proposed structural model was a good fit with the data set. The regression weight for each variable loading into its relevant latent variable was between 0.655 and 0.976, with critical ratios (t-value) greater than the minimum cut-off value of 1.96, which indicates that the relationships between each latent variable and its factors are statistically significant.

Hypothesis Testing

As highlighted before, the structural model can be tested to examine the hypothesised relationships between the constructs in the theoretical model (Kline, 2015). This section aims to test the relationships between the latent variables in the Smartphone password manager adoption model. As depicted in Figure 2, the model has a number of hypotheses focusing on the main construct “intention”, and four more hypotheses centring on the “perceived risk” and “dissatisfaction” constructs (those aligning with constraints). The SEM output reported in Table 11 was evaluated based on the path coefficient value, critical ratio CR (t-value) and p-value. The standard measures used to evaluate the significance of the relationships between the independent and dependent variables are CR values of at least 1.96, and $p \leq .05$ (Byre, 2013). As Table 11 shows, six of the hypotheses related to intention construct are supported, while two hypotheses are not supported. Hypotheses that are related to risk and dissatisfaction constructs are all supported. The hypothesis that tests the relationship between intention and actual adoption is supported.

Insert Table 11 About Here

Insert Figure 4 About Here

Phase 5: Discussion and Reflection

This section discusses the findings, which go towards answering the primary research question:

"Which Factors Influence Smartphone Password Manager Adoption?"

Our initial interviews, reported earlier, identified eight factors directly influencing the intention to adopt a password manager, namely: relative usefulness, response efficacy, perceived risk, dissatisfaction, monetary cost, learning cost, set-up cost and descriptive norms. However, the quantitative analysis of the data from this study revealed that only six factors significantly influence password manager adoption. These factors are related to the two constructs related to our initial constraints: (1) perceived risk related to passwords (security and privacy concerns), and (2) dissatisfaction with their existing practice (perceived vulnerability and the response cost). Furthermore, intention significantly predicts the actual adoption of a password manager. The final MIGRANT model, including only the significant factors, is depicted in Figure 5.

Insert Figure 5 About Here

Returning to the Constraints

Earlier, we mentioned two constraints on a model that could accurately model password manager adoption.

Mooring Factor: Perceived Risk:

Perceived risk (both security and privacy concerns) is an important barrier to those considering whether to switch to using a password manager. In this study, perceived risk was defined as the belief that, if they use a password manager, they could lose all their passwords. Some are also concerned that the service providers would be able access their passwords. The relationship between perceived risk and adoption intention indicates that those who consider password managers risky are less likely to adopt them.

A comparison of security and privacy concerns shows that security concerns have a greater impact on adoption than privacy concerns. These findings are similar to those of Yang et al. (2015). In a web-to-mobile shopping extension behaviour study, they concluded that the perceived risk of mobile shopping services might be an important factor in explaining the intention to install a mobile shopping extension. Moreover, according to a study by Gumussoy et al. (2018), when people perceive mobile banking to be risky and insecure, their intention to use mobile banking declines, consistent with the findings of this study.

Push Factor: Pre-Existing Password Management Routines:

Dissatisfaction with the way they are currently managing their passwords predicts the intention to adopt a password manager. Evidence of the influence of dissatisfaction on strengthening intention to switch to disruptive technology exists in the literature (Fan & Suh, 2014; Bhattacherjee & Park, 2014). Our study reveals that dissatisfaction with current password management routines is mainly due to response cost. Response cost is exacerbated by the sheer number of passwords people have for different accounts. They have to try to remember the correct password for

each of their accounts, or use a fallback authentication to reset their passwords. Even if users record their passwords in a notebook, or on their Smartphones as a contact, this means that they have to look it up each time they want to access an account. This is arduous, time consuming and risky.

Another source of dissatisfaction is the perception of being vulnerable to cyber attacks. As a means to cope with the cost of managing many passwords, people use coping skills which they know are insecure. This may well lead to dissatisfaction.

Other Influential Factors

Pull Factors: People's perceptions of the advantages of a password manager in improving their task performance, compared to not using it, predicts their intention to adopt. This is consistent with prior research. Bhattacherjee and Park (2014) found that relative usefulness could predict the intention to use cloud-based services. Similarly, it has been revealed that the relative usefulness of social networking services (SNS), as compared to blogs, influenced bloggers' intention to switch to SNS (Hsieh et al., 2011). It is important to emphasise the advantages of using a password manager in improving overall task performance, as compared to not using one, in order to foster an intention to adopt one.

Furthermore, perceptions of the efficacy of password managers in protecting passwords and online accounts influences people's intention to adopt a password manager. The role of perceived response efficacy in strengthening intention is also reported by other studies. For example, the effectiveness of SNS as an expression function of the account owners strengthens the willingness of bloggers to switch from traditional blogs to the use of SNS (Hsieh et al., 2011). Because password managers are not only a utility tool, but also act as a security measure, the effectiveness of this tool is particularly important in encouraging formulation of a behavioural intention to install a password manager. Moreover, prior information security studies have consistently suggested that perceived effectiveness could predict the motivation to perform security behaviours (Mou et al., 2017).

Mooring Factors: Password manager switching is deterred by a number of factors. Perceptions of the cost of setting up a password manager for the first time were found to be a strong deterrent. The setup process includes transferring existing password details and recording password changes, as well as remembering to record credentials for new accounts. As mentioned earlier, people already have their own routines for managing their passwords. Having many passwords for different accounts makes it a tedious and time-consuming process to move each of these accounts with their passwords to the password manager. This negative impact of set-up cost on intention is consistent with the findings of other scholars (Bhattacherjee and Park, 2014; Chang et al., 2014; Schreiner & Hess, 2015). Owing to the strong mooring effect of set-up cost, service providers should ease the set-up cost as much as possible. Allowing new users to easily transfer their login credentials to the password manager from browsers, and simplifying the sign-up process, would ease adoption.

Unexpectedly, learning cost is not a significant barrier to password manager adoption among Smartphone owners.

Many people are now using different mobile applications on their Smartphones, offering various services compared to using desktop or web-based applications. They might be used to interacting with different types of mobile applications, so do not dread the cost related to learning how to use a new one. Another explanation is that the availability of such apps on the 'Google Play Store' might reassure them of its ease of use.

Similarly, monetary cost is not a significant mooring factor. This might be due to the fact that some password manager applications are available free of charge. However, since the application is storing passwords, people might not trust the free versions, due to the common belief that the true cost of free services is a loss of privacy.

Descriptive Norms: A growing number of studies in the information security literature provide evidence that descriptive norms (social influence) influence the intention to perform information security-related behaviours (Bhattacherjee and Park, 2014; Chen et al., 2018). Our study confirmed the influence of descriptive norms in influencing the intention to adopt an innovative technology (Mour & Lin, 2015; Park & Ryoo, 2013). Perceptions of password managers being popular and widely adopted would influence the intention to adopt. Therefore, if a critical mass of people started using password managers, many more would probably follow suit, given the real and important influence of descriptive norms on adoption decisions.

Research Implications

This research has some practical and theoretical implications. First, the study employed migration theory to examine the factors influencing security behaviours from three different perspectives: pull, push and mooring factors. The research provides theoretical insights for researchers, which may assist in encouraging researchers to view security behaviour in a wider lens, and consider existing behaviours, as well as the new recommended behaviour. Second, the results of this study reveal some important factors related to password managers and adoption decisions, which have not been addressed by previous studies.

This study suggests that service providers and security advisors should consider focusing their promotion strategies more on establishing trust in password managers. For example, the source code of a password manager could be open and available to anyone to examine. Moreover, the cost of migrating accounts credentials to the password manager should be acknowledged and accommodated. Developers should focus attention on the ease of setting up their password manager. They could facilitate the importing of existing account credentials[5], instead of requiring people to move them manually. Illustrating the usefulness of password managers, compared to not using them, and their effectiveness in protecting online accounts, could help to encourage more people to adopt them. The power of social influence can also be utilised to encourage more people to start using password managers.

Limitations

This study recruited Android Smartphone owners via a social networking site. As such, the model might not accurately describe the factors influencing iPhone owners, for example. The Apple keychain is pre-installed on Apple devices, and device owners might well consider installation of another password manager to be superfluous. In this case, the push, pull and mooring factors might be different. It also has to be acknowledged that while we checked for a password manager installation while CyberPal was being used, we could not easily determine whether such installation actually converted to long-term use and adoption of the password manager. A longer-term study would have to be carried out to explore the factors that predict entrenched usage. Furthermore, the relationship between the intention and the actual adoption is mediated by the recommendation intervention within CyberPal (Alkaldi, 2019). However, in this study, we only measured the impact of intention on adoption, not the impact of the intervention participants were exposed to. Moreover, the result of the current study may lack generalizability as the data was collected from Facebook users and their friends.

Conclusions and Future Work

A password management application is one of the most empowering solutions to the password security and usability problem. The initial factors affecting password manager adoption decisions were identified based on a number of semi-structured interviews and confirmed using a Smartphone app as a survey harness. The study employed migration theory as a theoretical lens to explain Smartphone owners' password manager switching behaviours. Using SEM analysis, six factors were found to be significant in predicting adoption of a password manager: descriptive norms, relative usefulness, response efficacy, dissatisfaction, perceived risk and set-up cost. This study has contributed to the information security field by applying migration theory to understand password manager adoption behaviour. Furthermore, the study also confirmed that the intention to perform a security behaviour predicts actual security behaviours in this context. The study can also provide guidance to service providers and security advisors in effectively promoting the adoption of password managers.

Future research should focus on identifying the particular factors that would apply if migration theory were applied to other relatively poorly adopted security tools, such as Virtual Private Networks (Gangadharan et al., 2019), two factor authentication (Petsas et al., 2015) or security software on Smartphones (Mylonas et al., 2013).

References

Acheampong, P., Zhiwen, L., Antwi, H. A., Otoo, A. A. A., Mensah, W. G., & Sarpong, P. B. (2017). Hybridizing an Extended Technology Readiness Index with Technology Acceptance Model (TAM) to Predict E-Payment Adoption in Ghana. *American Journal of Multidisciplinary Research, 5*(2), 172–184.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40–46.

Agholor, S., Sodiya, A., Akinwale, A., Adeniran, O., & Aborisade, D. (2016). A Preferential Analysis of Existing Password Managers from End-Users' View Point. *International Journal of Cyber-Security and Digital Forensics, 5*(4):187– 196.

Ahuja, R., Ramrakhyani, M., Manchundiya, B., & Shroff, S. (2016). Dual Layer Secured Password Manager using Blowfish and LSB. *International Journal of Computer Applications, 143*(3), 5–10.

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

Al-Sinani, H. S., & Mitchell, C. J. (2010). Using cardspace as a password manager. In *IFIP Working Conference on Policies and Research in Identity Management*, (18–30), Oslo, Norway: Springer.

Alalwan, A. A., Baabdullah, A. M., Rana, N. P., Tamilmani, K., & Dwivedi, Y. K. (2018). Examining adoption of mobile Internet in Saudi Arabia: Extending TAM with perceived enjoyment, innovativeness and trust. *Technology in Society, 55*, 100–110.

Alkaldi, N. & Renaud, K.V. (2016). Why do people adopt, or reject, smartphone password managers? *In European Workshop on Usable Security (EuroUSEC)*, Darmstadt, Germany:Internet Society.

Alkaldi, Nora Abdullah (2019). *Adopting password manager applications among smartphone users*. PhD thesis, University of Glasgow.

Anderson, G. O. (2014) Identity theft: Who's at risk? *AARP Research*, September 26 https://www.aarp.org/research/topics/economics/info-2014/identity-theft-incidence-riskbehaviors.html Accessed 13 July.

Arias-Cabarcos, P., Marín, A., Palacios, D., Almenarez, F., & Díaz-Sanchez, D. (2016) Comparing password management´ software: Toward usable and secure enterprise authentication. *IT Professional, 18*(5), 34–40.

Aurigemma, S., Mattson, T., & Leonard, L. (2017). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications? In *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS)*, (4061–4070). Hawaii:University of Hawaii.

Aurigemma, S., Mattson, T., & Leonard, L. N. (2019). Evaluating the core and full protection motivation theory nomologies for the voluntary adoption of password manager applications. *AIS Transactions on Replication Research*, 5(1), paper 3.

Ayyagari, R., Lim, J., & Hoxha, O. (2019). Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers. *Contemporary Management Research, 15*(4), 227–245.

Bandura, A. (1986). *Social foundations of thought and action*. Prentice Hall, Englewood Cliffs, NJ.

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *Annual Review of Psychology, 52*(1), 1–26

Bandura, A., & Walters, R. H. (1977). *Social learning theory, volume 1*. Prentice-Hall, Englewood Cliffs, NJ.

Barbosa, N. M., Hayes, J., & Wang, Y. (2016). Unipass: design and evaluation of a smart device-based password manager for visually impaired users. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*, (49–60), Heidelberg, Germany: ACM.

Barn, B. S., Barn, R., & Tan, J.-P. (2014). Young people and smart phones: An empirical study on information security. In *47th Hawaii International Conference on System Sciences*, (4504–4514), Big Island, Hawaii:IEEE.

Barrett, P. (2007). Structural equation modelling: Adjudging model fit. *Personality and Individual Differences, 42*(5), 815–824.

Bhattacherjee, A. & Park, S. C. (2014). Why end-users move to the cloud: a migration-theoretic analysis. *European Journal of Information Systems*, 23(3), 357–372.

Bicakci, K., Atalay, N. B., Yuceel, M., & Van Oorschot, P. C. (2011). Exploration and field study of a password manager using icon-based passwords. In *International Conference on Financial Cryptography and Data Security,* (104–118), Gros Islet, Saint Lucia: Springer.

Bosnjak, L., & Brumen, B. (2019). Rejecting the death of passwords: Advice for the future. *Computer Science and Information Systems, 16*(1), 313–332.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D. & 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), 837–864.

Brettell, C. B., & Hollifield, J. F. (editors). *Migration theory: Talking across disciplines*. Oxon, UK: Routledge.

Butler, R., & Butler, M. (2015). The password practices applied by South African online consumers: Perception versus reality. *South African Journal of Information Management, 17*(1), 1–11.

Byrne, B. M. (2013). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. New York: Taylor & Francis Group, 2 edition.

Chang, I.-C., Liu, C.-C., & Chen, K. (2014). The push, pull and mooring effects in virtual migration for social networking sites. *Information Systems Journal*, 24(4), 323–346.

Chaudhary, S., Schafeitel-Tahtinen, T., Helenius, M. & Berki, E. (2019). Usability, security and trust in password man-¨ agers: A quest for user-centric properties and features. *Computer Science Review, 33*, 69–90.

Chen, X., Wu, D., Chen, L. & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management, 55*(8), 1049–1060.

Chiasson, S., van Oorschot, P. C. & Biddle, R. (2006). A usability study and critique of two password managers. In *USENIX Security Symposium*, pages 1–16, Vancouver, Canada:USENIX.

Cialdini, R. B., Reno, R. R. & Kallgren, C. A. (1990). A focus theory of normative conduct: recycling the concept of norms to reduce littering in public places. *Journal of Personality and Social Psychology, 58*(6), 1015–1026.

Couillard, K. (2019). Password security survey results - Part 1, 2015. March 6 (Roboform) https://roboformblog.siber.com/2015/03/06/password-security-survey-results-part-1/ Accessed 2 July.

Couillard, K. (2019). Password Security Survey Results- Part 2, 2015. March 6 (Roboform) https://roboformblog.siber.com/2015/03/13/password-security-survey-results-part-2/ Accessed 2 July.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. In *Proceedings NDSS, volume 14*, (23–26). San Diego, USA:Internet Society.

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results*. PhD thesis, Sloan School of Management, Massachusetts Institute of Technology.

Djeni, I & Erbilek, M. (2017). Intention to use biometric systems among international students in Cyprus. In *9th International Conference on Computational Intelligence and Communication Networks (CICN),* (229–235), Cyprus: IEEE.

Ernst, C.-P. H. (2015). Risk hurts fun: The influence of perceived privacy risk on social network site usage. In *Factors Driving Social Network Site Usage*, (45–56). Gabler, Wiesbaden: Springer.

Fagan, M., Albayram, Y., Khan, M. M. H. & Buck, R. (2017) An investigation into users' considerations towards using password managers. *Human-Centric Computing and Information Sciences*, 7(12), article 12.

Fan, L., & Suh, Y.-H. (2014). Why do users switch to a disruptive technology? An empirical study based on expectation disconfirmation theory. *Information & Management, 51*(2), 240–248.

Ferber, R. (1977). Research by Convenience. *Journal of Consumer Research, 4*(1), 57 – 58.

M. Fishbein & I. Ajzen. (2011). *Predicting and Changing Behavior: The Reasoned Action Approach*. New York, USA: Psychology Press.

Fornell, C. & Larcker, D. F. (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.

Fosnot, C. T. & Perry, R. S. (1996). Constructivism: A psychological theory of learning. *Constructivism: Theory, Perspectives, and Practice, 2*, 8–33.

Friendman, B. (2014*). A study of South African computer users' password usage habits and attitude towards password security*. Master's thesis, Department of Information Systems, Rhodes University.

Frimpong, K., Al-Shuridah, O., Wilson, A., & Sarpong, F. A.-A. (2017). Effect of inherent innovativeness and consumer readiness on attitudes to mobile banking. *Journal of Financial Services Marketing, 22*(4), 187–201.

Gallagher, E. A. (2019) Choosing the Right Password Manager. *Serials Review*, 45(15), 1-4.

Gangadharan, S., Dosono, B., Ngu, K., & Arbor, A. (2019). *Virtually Unused*. https://www.newamerica.org/oti/policy-papers/virtually-unused/ Accessed 1 July.

Gaskin, J. (2012). *Validity master*, http://statwiki.kolobkreations.com, Accessed 21 Nov 2017.

George, D. (2011). SPSS for windows step by step: A simple study guide and reference, 17.0 update, 10/e. Pearson Education, India.

Gray, J., Franqueira, V. N., & Yu, Y. (2016). Forensically-sound analysis of security risks of using local password managers. *In IEEE 24th International Requirements Engineering Conference Workshops (REW),* (114–121), Beijing, China: IEEE.

Gumussoy, C. A., Kaya, A. & Ozlu, E. (2018). Determinants of mobile banking use: an extended TAM with perceived risk, mobility access, compatibility, perceived self-efficacy and subjective norms. In *Industrial Engineering in the Industry 4.0 Era*, (225–238). Vienna, Austria: Springer.

Hair Jr, J. F., Anderson, R. E., Tatham, R. L. & Black, W. C. (2010). *Multivariate data analysis*, (7th ed.). Upper Saddle River, NJ, USA: Prentice-Hall.

Hale J. L., Householder, B. J. & Greene, K. L. (2002) The theory of reasoned action. The persuasion handbook: Developments in Theory and Practice, 14, 259–286.

Hanafizadeh, P., Keating, B. W. & Khedmatgozar, H. R. (2014). A systematic review of internet banking adoption. *Telematics and Informatics, 31*(3), 492–510.

Hoonakker, P., Bornoe, N., & Carayon, P. (2009). Password authentication from a human factors perspective: Results of a survey among end-users. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 53(6), (459–463), Los Angeles, CA: SAGE Publications.

Hooper, D., Coughlan, J., & Mullen, M. (2008). Structural equation modelling: Guidelines for determining model fit.

*Electronic Journal of Business Research Methods, 6(*1):53–60.
Hovav, A. & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*, 35–49.
Hsieh, Y.-C., Hsieh, J.-K. & Feng, Y.-C. (2011). Switching between social media: The role of motivation and cost. In *2nd International Conference on Economics, Business and Management*, volume 22, (92–96), Maldives.
Hu, S., Hu, B. & Cao, Y. (2018). The wider, the better? The interaction between the IoT diffusion and online retailers' decisions. *Physica A: Statistical Mechanics and its Applications*, 509, 196–209.
Ion, I., Reeder, R. & Consolvo, S. (2015). "... no one can hack my mind": Comparing expert and non-expert security practices. In *Eleventh Symposium on Usable Privacy and Security (SOUPS),* (327–346), Denver, Colorado: ACM
Johansson, S. (2016). *Introducing password managers into multiple-password environments*. Master's thesis, Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology.
Jost, J. T. (2015). Resistance to change: A social psychological perspective. *Social Research: An International Quarterly*, 82(3), 607–636.
Karole, A., Saxena, N. & Christin, N. (2010). A comparative usability evaluation of traditional password managers. In *International Conference on Information Security and Cryptology*, (233–251), Shanghai, China: Springer.
Kim, B. (2010). An empirical investigation of mobile data service continuance: Incorporating the theory of planned behavior into the expectation–confirmation model. *Expert Systems with Applications, 37*(10), 7033–7039.
Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008) A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems, 44*(2), 544–564.
Kim, D. J., Steinfield, C. & Lai, Y.-J. (2008) Revisiting the role of web assurance seals in business-to-consumer electronic commerce. *Decision Support Systems, 44*(4), 1000–1015.
Kline, R. B. (2015) *Principles and practice of structural equation modeling*. Guilford publications, New York.
Koppel, R., Blythe, J., Kothari, V. & Smith, S. (2016). Beliefs about cybersecurity rules and passwords: A comparison of two survey samples of cybersecurity professionals versus regular users. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*. Denver, Colorado: USENIX.
Kosë, A. (2009). Determination of reasons affecting the use of internet banking through logistic regression analysis. Journal of Global Strategic Management, 3(2), 67–76.
Lebek, B., Uffen, J., Neumann, M., Hohler, B. & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), 1049–1092.
Lee, E. S. (1966). A theory of migration. *Demography, 3*(1), 47–57.
Lee, J.-M. & Rha, J.-Y. (2016). Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior, 63*, 453–462.
Lee, Y. & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt antimalware software. European *Journal of Information Systems, 18*(2), 177–187.
Leon, J. F. Ten tips to combat cybercrime. *The CPA Journal,* 78(5), 6,8–11.
Li, H. & Evans, D. (2017). Horcrux: A password manager for paranoids. arXiv preprint arXiv:1706.05085.
Li, Y., Wang, H. & Sun, K. (2017) BluePass: A Secure Hand-Free Password Manager. In *International Conference on Security and Privacy in Communication Systems*, (185–205), Singapore, Singapore: Springer.
Li, Z., He, W., Akhawe, D. & Song, D. (2014). The emperor's new password manager: Security analysis of web-based password managers. In *23rd USENIX Security Symposium (USENIX Security 14*), (465–479), San Diego.
Little, R. J. (1988) A test of missing completely at random for multivariate data with missing values. Journal of the *American Statistical Association*, *83*(404), 1198–1202.
Lu, J., Yao, J. E. & Yu, C.-S. (2005). Personal innovativeness, social influences and adoption of wireless Internet services via mobile technology. *The Journal of Strategic Information Systems*, 14(3), 245–268.
Luevanos, C., Elizarraras, J., Hirschi, K. & Yeh, J.-h. (2017). Analysis on the security and use of password managers. In 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), (17–24), Taipei, Taiwan: IEEE.
Lyastani, S. G., Schilling, M., Fahl, S., Bugiel, S. & Backes, M. (2017). Studying the impact of managers on password strength and reuse, arXiv preprint arXiv:1712.08940.
Machuletz, D., Sendt, H., Laube, S., & Bohme, R. (2016). Users protect their privacy if they can: Determinants of webcam¨ covering behavior. In European Workshop on Usable Security (EuroUSEC), Darmstadt, Germany :Internet Society.
Maclean, R. & Ophoff, J. (2018). Determining Key Factors that Lead to the Adoption of Password Managers. In International Conference on Intelligent and Innovative Computing Applications (ICONIC), (1–7), Mauritius, IEEE.
Maduku, D. K. (2013). Predicting retail banking customers' attitude towards Internet banking services in South Africa. *Southern African Business Review, 17*(3), 76–100.

Martínez-Roman, J. A. & Romero, I. (2017). Determinants of innovativeness in SMEs: disentangling core innovation and technology adoption capabilities. *Review of Managerial Science, 11*(3), 543–569.
McCarney, D. (2013). *Password managers: Comparative evaluation, design, implementation and empirical analysis.* Master's thesis, Computer Science, Carleton University.
McGrath, R. G. (2013). The Pace of Technology Adoption is Speeding Up. *Harvard Business Review, 25*. https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up (Accessed 14 July 2019).
Morgan, R. M. & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing, 58*(3), 20–38.
Mou, J., Cohen, J. & Kim, J. (2017). A meta-analytic structural equation modeling test of protection motivation theory in information security literature. In *International Conference on Information Systems (ICIS): Transforming Society with Digital Innovation*, (1–20), Seoul, South Korea: AIS.
Mou, Y. & Lin, C. A. (2015). Exploring podcast adoption intention via perceived social norms, interpersonal communication, and theory of planned behavior. *Journal of Broadcasting & Electronic Media, 59*(3), 475–493.
Mwagwabi, F. (2015). *A Protection Motivation Theory approach to improving compliance with password guidelines*. PhD thesis, School of Engineering and Information Technology, Murdoch University.
Mylonas, A., Kastania, A. & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security, 34*, 47–66.
Nagin, D. S. & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology, 39*(4), 865–892.
National Cyber Security Centre. (2017). *What does the NCSC think of password managers?* National Cyber Security Centre. https:// www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers Accessed 2 July 2019.
Ngoqo, B. & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *Computers & Security, 53*:132–142.
Oliveira, T., Thomas, M., Baptista, G. & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior, 61*:404–414.
Park, S. C. & Ryoo, S. Y. (2013). An empirical investigation of end-users' switching toward cloud computing: A two factor theory perspective. *Computers in Human Behavior, 29*(1), 160–170.
Patil, S., Wasnik, K. & Bagade, S. (2019) Pen-Drive Based Password Management System for Online Accounts. In *Emerging Technologies in Data Mining and Information Security*, (693–704). Singapore: Springer.
Pearman, S., Zhang, S. A., Bauer, L., Christin, N. & Cranor, L. F. (2019) Why people (don't) use password managers effectively. In Fifteenth Symposium On Usable Privacy and Security (SOUPS). , (319–338), Santa Clara, CA: USENIX Association.
Petsas, T., Tsirantonakis, G., Athanasopoulos, E. & Ioannidis, S. (2015). Two-factor Authentication: Is the World Ready?: Quantifying 2FA Adoption. In *Proceedings of the Eighth European Workshop on System Security, EuroSec* '15, (4:1–4:7), Bordeaux, France:ACM.
Pew Research. (2017). *Americans and cybersecurity*. https://www.pewinternet.org/wp-content/ uploads/sites/9/2017/01/Americans-and-Cyber-Security-final.pdf Accessed 14 July 2019.
Pham, H., Brennan, L. & Richardson, J. (2017). Review of behavioural theories in security compliance and research challenge. In The *Proceedings of The Informing Science and Information Technology Education Conference*, (65–76), Vietnam: Informing Science Institute.
Ramayah, T., Rouibah, K., Gopi, M. & Rangel, G. J. (2009). A decomposed theory of reasoned action to explain intention to use Internet stock trading among Malaysian investors. *Computers in Human Behavior, 25*(6), 1222–1230.
Renaud, K., & Ophoff, J. (2019). Modeling inertia causatives: validating in the password manager adoption context. In 2019 Dewald Roode Workshop on Information Systems Security Research, IFIP Working Group 8.11/11.13, Bossier City, Louisiana: AIS.
Renaud, K., Otondo, R., & Warkentin, M. (2019). "This is the way 'I' create my passwords"... does the endowment effect deter people from changing the way they create their passwords? *Computers & Security, 82*, 241–260.
Renaud, K., & Zimmermann, V. (2019). Encouraging password manager use. *Network Security. June*, page 20.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114.
Roselius, T. (1971). Consumer rankings of risk reduction methods. *Journal of Marketing, 35*(1), 56–61.
Schechter, S. (2019). Before you use a password manager. https://medium.com/@stuartschechter/ before-you-use-a-password-manager-9f5949ccf168 Accessed 15 July 2019.
Schneier, B. (2014). Security of Password Managers. https://www.schneier.com/blog/archives/2014/09/security_of_pas.html Accessed 2 July 2019.

Schougaard, D., Dragoni, N. & Spognardi, A. (2016). Evaluation of professional cloud password management tools. *In International Conference on Web Engineering*, (16–28), Lugano, Switzerland: Springer.

Schreiner, M. & Hess, T. (2015). Examining the role of privacy in virtual migration: The case of WhatsApp and Threema.*In Proceedings of the 21st Americas Conference on Information Systems, AMCIS '15*, (paper 33), Fajardo, Puerto Rico: AIS.

Seiler-Hwang, S., Arias-Cabarcos, P., Marín, A. Almenares, F., Díaz-Sanchez, D. & Becker, C. (2019). "I don't see why I would ever want to use it. Analyzing the Usability of Popular Smartphone Password Managers. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, (1937–1953), London: ACM.

Silver, D., Jana, S., Boneh, D., Chen, E., & Jackson, C. (2014). Password managers: Attacks and defenses. In *23rd USENIX Security Symposium*, (449–464), San Diego, California:USENIX.

Skog, B. (2002). 16 Mobiles and the Norwegian teen: identity, gender and class. In J. E. Katz and M. Aakhus, editors, *Perpetual contact: Mobile Communication, Private Talk, Public Performance*, (255–273). Cambridge, UK: Cambridge University Press.

Slade, E. L., Dwivedi, Y. K., Piercy, N. C. & Williams, M. D. (2015). Modeling consumers' adoption intentions of remote mobile payments in the United Kingdom: extending UTAUT with innovativeness, risk, and trust. *Psychology & Marketing, 32*(8), 860–873.

Sommestad, T., Hallberg, J., Lundholm, K. & Bengtsson, J. (2014). Variables influencing information security policy compliance: a systematic review of quantitative studies*. Information Management & Computer Security, 22*(1), 42– 75.

Stobert, E. & Biddle, R. (2014). The password life cycle: user behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security (SOUPS),* (243–255), Menlo Park, California:ACM.

Stobert, E. & Biddle, R. (2015). Expert password management. In *International Conference on Passwords*, (3–20), Cambridge, UK: Springer.

Sun, Y., Liu, D., Chen, S., Wu, X., Shen, X.-L. & Zhang, X. (2017). Understanding users' switching behavior of mobile instant messaging applications: An empirical study from the perspective of push-pull-mooring framework. *Computers in Human Behavior, 75*, 727–738.

Tabachnick, B. G., Fidell, L. S. & Ullman, J. B. (2013). *Using multivariate statistics*, sixth edition. Pearson, Boston, MA.

Tamil, E. M., Othman, A. H., Abidin, S. A. Z., Idris, M. Y. I. & Zakaria, O. (2007). Password Practices: A Study on Attitudes towards Password Usage among Undergraduate Students in Klang Valley, *Malaysia. Journal of Advancement of Science & Arts, 3*, 37–42.

Thakur, R., Angriawan, A. & Summey, J. H. (2016). Technological opinion leadership: The role of personal innovativeness, gadget love, and technological innovativeness. *Journal of Business Research, 69*(8), 2764–2773.

Tu, Z., Yuan, Y. & Archer, N. (2014). Understanding user behaviour in coping with security threats of mobile device loss and theft. International *Journal of Mobile Communications, 12*(6), 603–623.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N. & Cranor, L. F. (2015). "I Added '!' at the End to Make It Secure": Observing Password Creation in the Lab. In Eleventh Symposium on Usable Privacy and Security (SOUPS), (123–140), Ottawa, Canada:ACM.

Vafaei-Zadeh, A., Ramayah, T., Wong, W. P. & Hanifah, H. Md. (2018). Modelling internet security software usage among undergraduate students: A necessity in an increasingly networked world. *VINE Journal of Information and Knowledge Management Systems, 48*(1), 2–20.

Vasileiadis, A. (2014). Security concerns and trust in the adoption of m-commerce. *Social Technologies, 4*(1), 179–191.

Von Zezschwitz, E., De Luca, A., & Hussmann, H. (2014). Honey, I shrunk the keys: influences of mobile devices on password composition and authentication performance. In *Proceedings of the 8th Nordic Conference on Human Computer Interaction: Fun, Fast, Foundational*, (461–470), Helsinki, Finland: ACM.

Wang, L., Li, Y. & Sun, K. (2016). Amnesia: A bilateral generative password manager. In *36th International Conference on Distributed Computing Systems (ICDCS)*, (313–322), Nara, Japan:IEEE.

Wash, R., Rader, E., Berman, R. & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. In *Twelfth Symposium on Usable Privacy and Security (SOUPS),* (175– 188), Denver, Colorado: ACM.

Woon, I., Tan, G.-W. & Low, R. (2005). A protection motivation theory approach to home wireless security. In *ICIS Proceedings*, (367–380), Las Vegas, USA: AIS.

Yang, S., Chen, Y. & Wei, J. (2015). Understanding consumers' web-mobile shopping extension behavior: A trust transfer perspective. *Journal of Computer Information Systems, 55*(2), 78–87.

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2013). Password advice shouldn't be boring: Visualizing password guessing attacks. In *APWG eCrime Researchers Summit*, (1–11), San Francisco, California: IEEE.
Zhang-Kennedy, L., Chiasson, S., & van Oorschot, P. (2016). Revisiting password rules: facilitating human management of passwords. In *APWG symposium on electronic crime research (eCrime),* (1–10), Toronto, Canada: IEEE.
Zhao, R., Yue, C. & Sun, K. (2013). Vulnerability and risk analysis of two commercial browser and cloud based password managers. *ASE Science Journal, 1*(4), 1–15.
Zhou, T. (2012). Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk. *Journal of Electronic Commerce Research, 13*(2),135–144.
Zhu, W. (2000). Which should it be called: Convergent validity or discriminant validity? *Research Quarterly for Exercise and Sport, 71*(2),190–194.

About the Authors

Nora Alkaldi is an Assistant Professor in Computer Science at the College of Computer and Information Science at King Saud University, Saudi Arabia. She received her Ph.D. in Computer Science from the University of Glasgow, U.K, in 2019. Her current research interests are human-centred security and privacy and usable security. Email: naalkaldi@ksu.edu.sa

Karen Renaud is a Scottish computing Scientist at the University of Strathclyde in Glasgow, working on all aspects of Human-Centred Security and Privacy. She is particularly interested in deploying behavioural science techniques to improve security behaviours, and in encouraging end-user privacy-preserving behaviours. Her research approach is multi-disciplinary, essentially learning from other, more established, fields and harnessing methods and techniques from other disciplines to understand and influence cyber security behaviours. She is a Visiting Professor at Rhodes University in South Africa and at Abertay University in the UK. She is also Professor Extraordinaire at the University of South Africa. Email: karen.renaud@strath.ac.uk

Notes

[1] Little's MCAR test is a mechanism used to examine the randomness of the missing data. Missing data are MCAR when the probability of missing data on a variable is unrelated to any other measured variable and is unrelated to the variable with missing values itself (Little, 1988).
[2] Data normality is considered an important assumption for further statistical analysis. Non-normality of the data is indicated when the data are either highly skewed or when there is kurtosis, which renders some statistical tests inaccurate and produces random effects in the results. (If the skewness value is greater than 2, then the data are positively (right) skewed, while if it is less than -2 they are negatively (left) skewed (George, 2011). Likewise, if the absolute overall kurtosis score is 2 or less, then there is no kurtosis (George, 2011). The non-normality is more often interpreted by the existence of outlier cases in the dataset. An outlier is a case in the collected data with an extreme value on one variable.
[3] Linearity is the existence of a linear relationship between the dependent and independent variables in the model. Homoscedasticity describes the case where the variance of the dependent variables is the same across all the levels of the independent data.
[4] Multicollinearity can be detected in the data when two different variables share a high correlation (≥0.90).
[5] As do KeeperSecurity, for example https://keepersecurity.com/

APPENDIX A

Table A.1. Measurement Item Descriptions

Construct	Definition	Measurement items
Pull Factors		
H1: Relative Usefulness (Bhattacherjee & Park, 2014)	The degree to which people believe that adopting a password manager will improve their task performance compared to existing password management routines	1. Using a Password Manager will help me accomplish my tasks more quickly than my current method for managing my passwords. 2. Using a Password Manager will improve my performance as compared to my current method for managing my passwords. 3. Using a Password Manager will enhance my effectiveness more than my current method for managing my passwords. 4. I will find using a Password Manager to be more useful than my current method for managing my passwords.
H2: Perceived Response Efficacy (Boss et al., 2015)	The belief that using password manager will be effective in improving password security and hence reducing the risk of online accounts being compromised or hacked.	1. Password manager application works for protecting my passwords from being stolen (Leon, 2018) and abused by attackers. 2. Password manager application is effective solution for protecting my passwords from being stolen and abused by attackers. 3. When using a password manager application, my passwords are more likely to be protected from being stolen and abused by attackers.
Push Factors		
H3: Dissatisfaction (Bhattacherjee & Park, 2014)	The degree to which people are dissatisfied with their current way for managing their passwords	How do you feel about your overall experience with the current method for managing your passwords? 1. Extremely dissatisfied... Extremely satisfied. 2. Extremely unpleasant... Extremely pleasant. 3. Extremely terrible... Extremely delightful
H3.a: Perceived vulnerability (Mwagwabi, 2015)	The degree to which a user believes that they are likely to experience password related threats	1. There is a chance that someone could successfully guess at least one of my passwords 2. There is a chance that someone could successfully crack at least one of my passwords using password cracking software 3. There is a chance that someone could hack into at least one of my important email accounts 4. If someone hacked into my important email account there is a chance that they could guess my other important passwords

Construct	Definition	Measurement items
H3.b: Response cost (Woon et al., 2005)	User perception about the cost of managing passwords without password manager	1. Managing my passwords currently requires a considerable investment in Time. 2. Currently, there are too many overheads associated with Managing my passwords. 3. Managing my passwords currently requires a considerable effort other than time. 4. Managing my passwords currently causes problems such as memorability issues and task delay
Mooring Factors		
H4: Perceived Risk (Zhou, 2012)	The degree to which people believe that if they use a password manager, they will suffer from potential problems such as losing all their passwords.	1. Providing password manager with my passwords would involve many unexpected problems. 2. It would be risky to put my passwords in a password manager. 3. There would be high potential for loss in saving my passwords in a password manager.
H4.a: Security Concern (Kim et al., 2008)	Perceptions about the security of password manager applications	1. Password managers implement security measures to protect my passwords from being hacked (R). 2. Password managers usually ensure that transferring information is protected from hacking attacks (R). 3. I feel safe in saving my passwords on password managers (R). 4. I feel secure in managing my passwords using password managers (R)
H4.b: Privacy Concern (Ernst, 2015)	Concerns about the probability of having passwords and personal information disclosed as a result of using a password manager	1. Using a password manager leads to a loss of control over the privacy of my passwords and personal data. 2. Using a password manager allows others to view my passwords and personal data. 3. Overall I see a privacy threat linked to password manager's usage.
H5: Learning cost (Bhattacherjee & Park, 2014)	The perceived effort and time needed to learn how to use a password manager and get used to it	1. It will take me a lot of time to learn to use a Password Manager's features. 2. It will take me a lot of effort to get up to speed and use a Password Manager. 3. Learning to use a Password Manager well will be difficult.
H6: Set-up cost (Bhattacherjee & Park, 2014)	The perceived effort and time required to set up the password manager and start using it	1. It will take a lot of time to set up my device and online accounts to use a Password Manager. 2. It will take a lot of effort to set up my device and online accounts to use a Password Manager. 3. Overall, the process involved in setting up a Password Manager is very elaborate.

Construct	Definition	Measurement items
H7: Monetary Cost (Kim, 2010)	The monetary costs related to purchasing a password manager.	1. The fee that I have to pay for the use of a password manager would be too high. 2. The fee that I have to pay for the use of a password manager would be reasonable (R). 3. I would be pleased with the fee that I have to pay for the use of a password manager (R).
Other Factors		
H8: Descriptive Norm (Ramayah et al., 2009)	Perceptions about whether others in their social or personal networks are using password manager or not.	1. Most of my friends are using a Password Manager. 2. Most of my family members are using a Password Manager. 3. Most of my co-workers are using a Password Manager. 4. Most people I know are using a Password Manager.
H9: Intention (Boss et al., 2015)	The extent to which the user plans to use a password manager in the near future	1. I intend to use a password manager within a week. 2. I predict I will use a password manager within a week. 3. I plan to use a password manager within a week.
Control Factors		
Exposure to hacking (Mwagwabi, 2015)	Prior exposure to a hacking incident experienced by either the user or someone they know personally and the degree to which the experience affected them.	1. Have you ever had an important email account a social networking account an online shopping account or online banking account hacked? (Yes, No). 2. Please indicate the degree to which that experience affected you (in terms of lost data, lost time, monetary losses, identity theft etc.) 3. Has someone you know personally ever had their important email account, social network account, online shopping account or online banking account, hacked into? (Yes, No). Please indicate the degree to which that experience affected you (in terms of lost, data, lost time, monetary losses, identity theft etc.)
Innovativeness (Lee and Rha, 2016)	The degree to which the user is relatively early in adopting new technologies than others in their community	1. Other people come to you for advice on new technologies. 2. In general, you are among the first in your circle of friends to acquire new technology when it appears. 3. You can usually figure out new high-tech products and services without help from others.
Adoption behaviour	The actual adoption of a password manager	Regularly retrieving all the applications installed on the person's phone device and checking for an installed password manager application

Table A.2. Correlation Matrixes

	HACK	DISSAT	PVUL	RCMAN	RU	PWMREFF	INNOV	DNORM	INT	PMFEE	PWMSETC	PWMLC	PMSEC	PRISK	PWMPRV
HACK	1														
DISSAT	.400**	1													
PVUL	.213**	.297**	1												
RCMAN	.305**	.377**	.257**	1											
RU	.299**	.529**	.181*	.458**	1										
PWMREFF	.297**	.560**	.236**	.374**	.667**	1									
INNOV	.298**	.353**	.063	.350**	.367**	.422**	1								
DNORM	.395**	.489**	.204**	.306**	.569**	.556**	.387**	1							
INT	.437**	.657**	.260**	.419**	.713**	.723**	.462**	.687**	1						
PWMFEE	-.185**	-.209**	-.073	-.094	-.299**	-.289**	-.124	-.365**	-.379**	1					
PWMSETC	-.323**	-.598**	-.233**	-.334**	-.556**	-.582**	-.367**	-.601**	-.833**	.453**	1				
PWMLC	-.278**	-.517**	-.195**	-.308**	-.495**	-.554**	-.660**	-.522**	-.627**	.283**	.622**	1			
PWMSEC	-.212**	-.343**	-.219**	-.208**	-.514**	-.557**	-.277**	-.500**	-.579**	.302**	.571**	.471**	1		
PRISK	-.350**	-.553**	-.178*	-.245**	-.622**	-.627**	-.347**	-.637**	-.802**	.381**	.787**	.606**	.669**	1	
PWMPRIV	-.230**	-.455**	-.086	-.130	-.448**	-.419**	-.192**	-.347**	-.583**	.222**	.602**	.464**	.369**	.700**	1

(**. Correlation is significant at the 0.01 level (2-tailed). *. Correlation is significant at the 0.05 level (2-tailed).)

Table A.3. Abbreviations

HACK	Exposure to Hacking	PWM REFF	Response Efficacy	PWM SETC	Setup Cost	DISSAT	Dissatisfaction
INNOV	Innovativeness	PRISK	Perceived Risk	PVUL	Perceived Vulnerability	DNORM	Descriptive Norms
PWM PRIV	Privacy Concerns	RC MAN	Response Cost	INT	Intention	PWMLC	Learning Cost
RU	Relative Usefulness	PWM FEE	Monetary Cost	PWM SEC	Security Concerns		

Table C.1. Standardized Regression Weights

Construct	#	C.R (t-val)	Factor L'ding
H1:	1	*	.867
Relative	2	14.733	.824
Usefulness	3	14.748	.824
	4	16.536	.880
H2:	1	*	.899
Response	2	19.372	.917
Efficacy	3	16.148	.836
H3:	1	*	.866
Dissatisfaction	2	16.993	.901
	3	16.423	.881
H3.a:	4	*	.849
Perceived	3	14.644	.848
Vulnerability	2	14.753	.852
	1	14.670	.849
H3.b:	1	*	.857
Response Cost	2	16.337	.887
	3	15.576	.862
	4	15.068	.845
H4:	1	*	.933
Perceived Risk	2	25.797	.942
	3	26.328	.947
H4.a:	1	*	.817
Security	2	13.910	.851
Concerns	3	13.723	.842
	4	13.709	.842
H4.b:	3	*	.849
Privacy	2	16.827	.912
Concerns	1	16.179	.888

Construct	#	C.R (t-val)	Factor L'ding
H5:	1	*	.850
Learning Cost	2	13.638	.815
	3	14.079	.833
H6:	1	*	.930
Setup Cost	2	23.039	.919
	3	24.367	.934
H7:	3	*	.923
Monetary Cost	2	20.902	.928
	1	17.274	.845
H8:	1	*	.914
Descriptive	2	24.548	.944
Norms	3	26.251	.962
	4	27.837	.976
H9:	1	*	.902
Intention	2	21.137	.919
	3	20.005	.900
Innovativeness	3	*	.923
	2	20.757	.906
	1	21.094	.911
Exposure to Hacking	2	*	.828
	1	6.585	.655

Table A.4. Discriminant Validity (*Values in bold represent the square root of AVE in Table 8) (Abbreviations in Table B.1)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PRISK	0.941														
INT	-0.850	0.907													
PVUL	-0.190	0.284	0.850												
PWMFEE	0.403	-0.404	-0.081	0.899											
INNOV	-0.365	0.491	0.070	-0.126	0.913										
PWMPRIV	0.752	-0.632	-0.092	0.244	-0.204	0.883									
PWMSEC	0.718	-0.631	-0.242	0.330	-0.298	0.399	0.838								
PWMSETC	0.825	-0.884	-0.251	0.480	-0.388	0.642	0.614	0.928							
DISSAT	-0.587	0.708	0.323	-0.222	0.379	-0.491	-0.370	-0.641	0.883						
PWMREFF	-0.669	0.779	0.263	-0.308	0.460	-0.460	-0.616	-0.623	0.612	0.885					
RCMAN	-0.261	0.457	0.282	-0.091	0.375	-0.139	-0.228	-0.354	0.410	0.409	0.863				
RU	-0.664	0.769	0.196	-0.330	0.381	-0.491	-0.563	-0.593	0.565	0.726	0.504	0.849			
PWMLC	0.666	-0.699	-0.221	0.312	-0.726	0.517	0.531	0.687	-0.581	-0.616	-0.346	-0.554	0.833		
DNORM	-0.666	0.723	0.209	-0.376	0.407	-0.375	-0.532	-0.624	0.512	0.592	0.321	0.606	-0.576	0.949	
Hack	-0.431	0.549	0.236	-0.248	0.329	-0.301	-0.254	-0.405	0.498	0.376	0.345	0.352	-0.333	0.462	0.747

Appendix B

Semi-structured Interview Questions

Demographic Data

Q1. *How old are you?* (18-24, 25-34, 35-44, 45-54, 55-64, 65-74, 75 or older, or Prefer not to say)

Q2. *What is your gender?* (Male / Female / Prefer not to say)

Q3. *What is the highest degree or level of school you have completed?*

Smartphone Usage and Password Experience

Q1. *What is your Smartphone operating system?*

Q2. *Do you use screen lock mechanism on your Smartphone (e.g. PIN and fingerprint)?*

If yes: (1) *What type of locking mechanism do you use on your Smartphone?* (2) *Why do you prefer this particular locking mechanism?*

If No: (1) *Why do you not think you need a locking mechanism?*

Q3. *On a typical day, how many passwords do you enter on your Smartphone?*

Q4. *Have you ever bought anything via your Smartphone?*

Q5. *How do you manage your passwords?*

Q6. *Do you ever use the same password for two or more accounts?*

If Yes: *Why do you think people use the same password for two or more accounts?*

Q7. *How many times did you use password recovery/reset mechanisms in the last 6 months (e.g. 'forget my password' functionality)?*

Q8. *Do you write down your passwords somewhere?*

Q9. *Do you save your passwords in the web browser in your device (ie: when you access your account on a website, it automatically fills in your details?*

Password Manager

A password manger is software that stores and organises passwords securely. It automatically populates passwords for you. Most of them require one strong password or a fingerprint. (Examples: LastPass, 1Password,Dashlane)

Q1. *Do you use a Password Manger?*

If Yes: (1) *What password manger do you currently use?* (2) *Why did you choose this particular password manager?*

Q2. *What do you think the advantages would be of using a password manager application on your Smartphone?*

Q3. *What do you think the disadvantages would be of using a password manager application on your Smartphone?*

Q4. *Who are the important people in your life (think about the people you would like to be happy about what you do, or people you do not want to disappoint) only give their relationship to you ?*

Q5. *When you think about the people you mentioned above. Which of them will be happy that you are using password manager application on your phone?*

Q6. *When you think about the people you mentioned above. Which of them will not be happy that you are using password manager application on your phone?*

Q7. *Who do you get security advice from?*

If No in Q1: Q8. *Is there anything specific that prevents you from using a password manager on your phone?*

Q9. *What will make it possible or easy for you to use password manager application on your phone?*

If Yes in Q1: Q8. *Do you think there are any difficulties or barriers to using password manager applications on your phone?*

Q9. *What would make the password manager application you use better?*

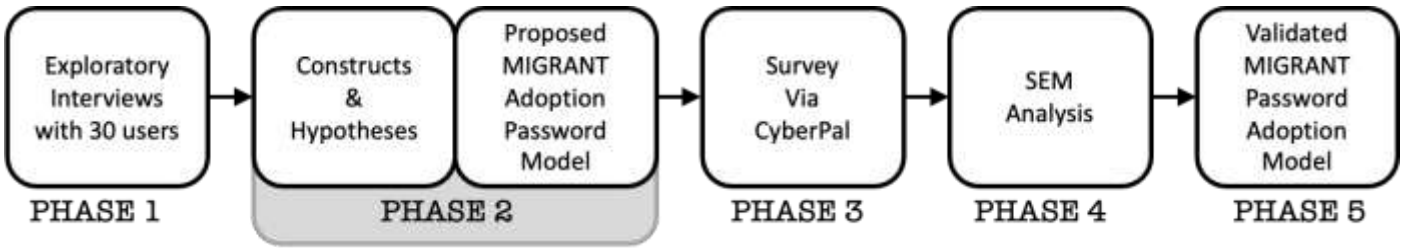

Figure 1. Research Phases

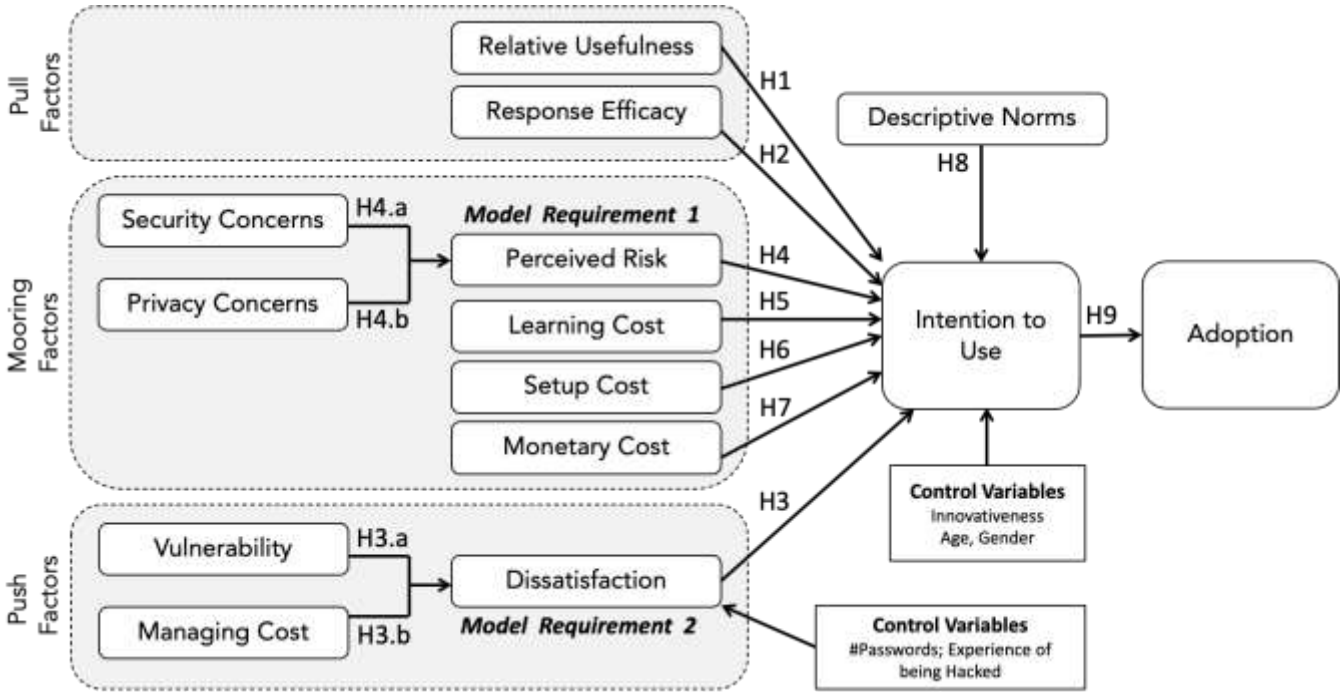

Figure 2. The Proposed Conceptual Model with Hypotheses

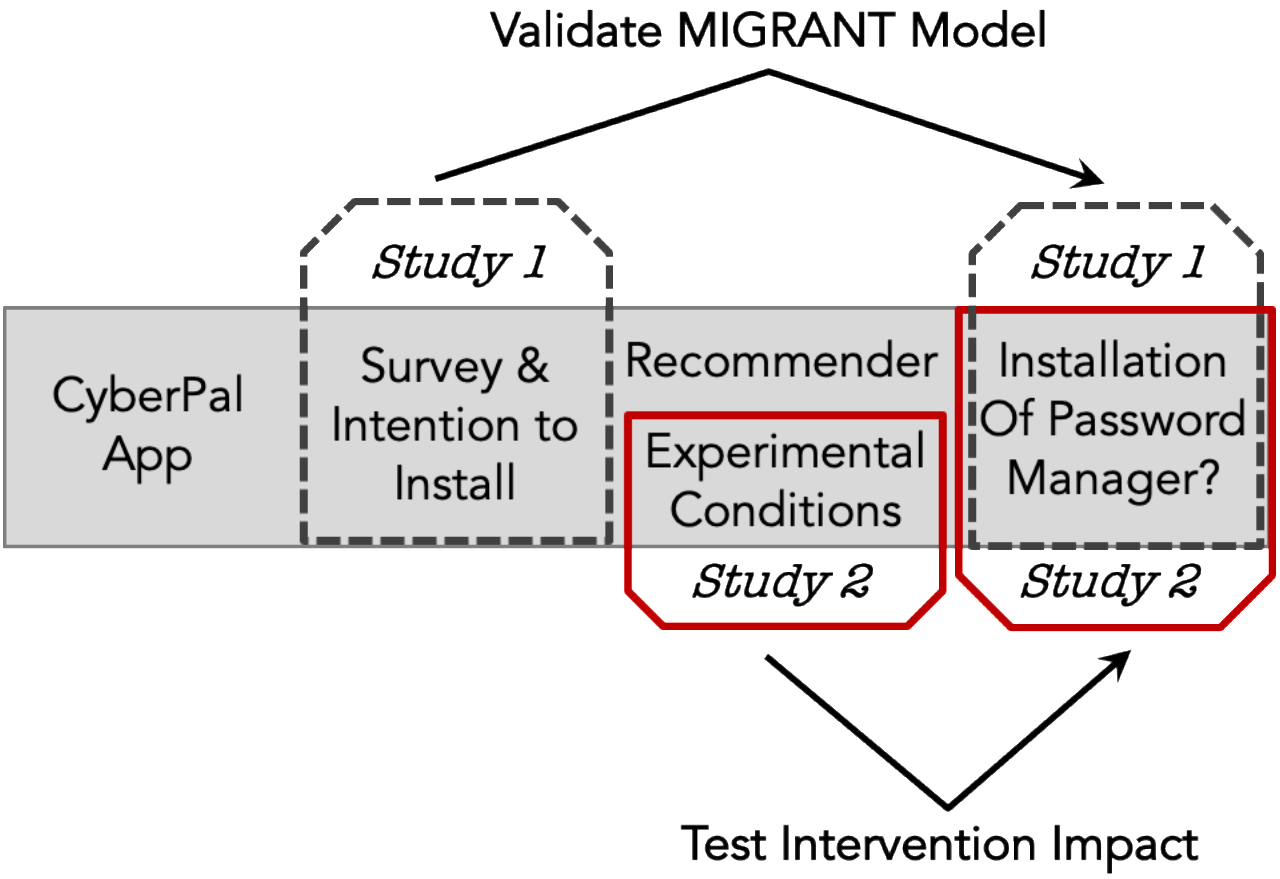

Figure 3. The CyberPal App support for Study 1 and Study 2

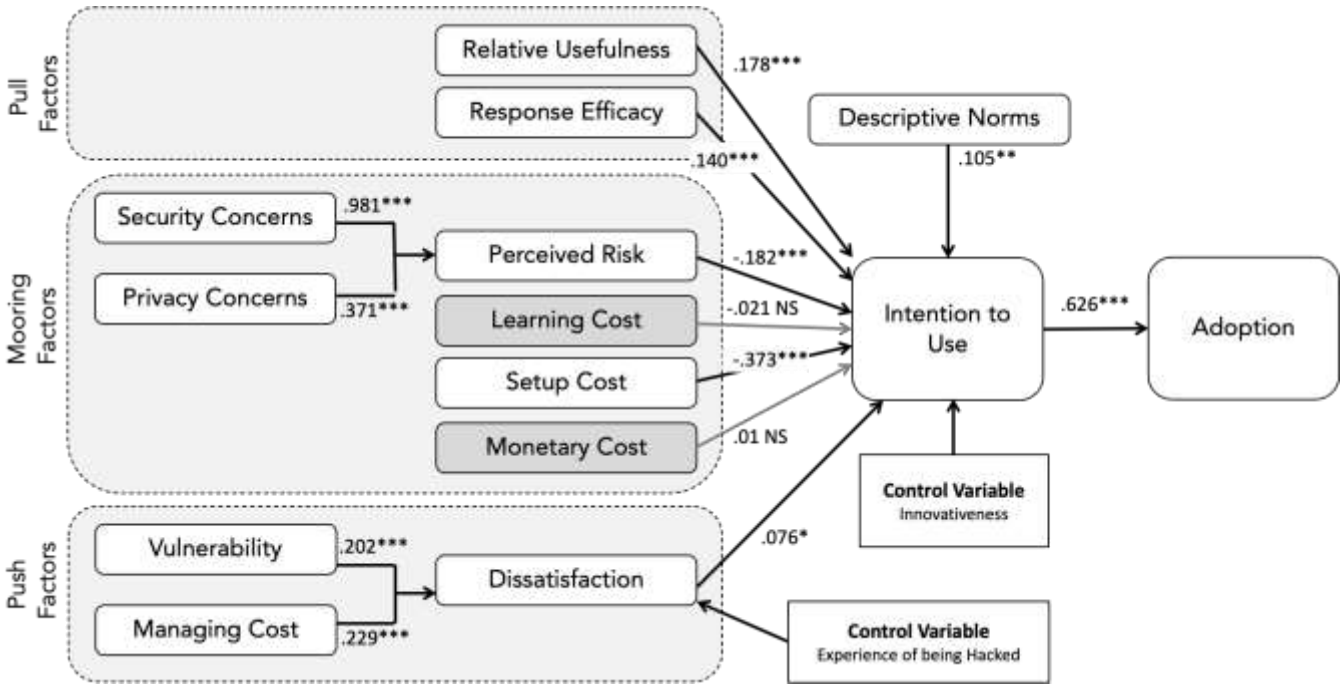

Figure 4. Demonstrating which associations are either supported, or not
[Significance denoted with * (*p<.001, **p<.005, *p<.05)]**

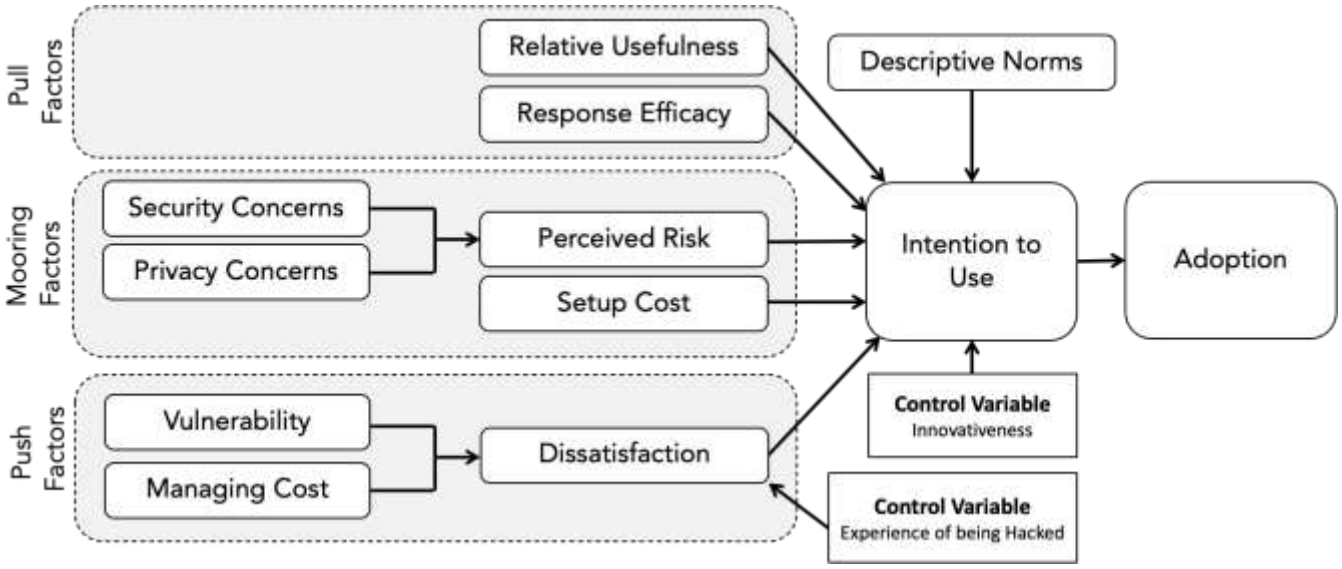

Figure 5. The Validated MIGRANT (MIGRation pAssword maNager adopTion) Model

Table 1. A Snapshot of Password Manager Adoption Rates (2007-2019)

Authors	Year	# Participants	Demographic	PM Usage
Tamil *et al.* [122]	2007	192	Malaysians	1%
Hoonaker *et al.* [56]	2009	836	employees	1%
Zhang-Kennedy *et al.* [134]	2013	21	university community	10%
			university community	18%
Anderson [9]	2014	2250	Americans	7%
Stobert and Biddle [118]	2014	27	university community	0%
Das *et al.* [35]	2014	224	university community	6%
Friendman [45]	2014	117	South Africans	15%
Stobert and Biddle [119]	2015	15	security experts	40%
Roboform [32, 33]	2015	1000	general public	8%
Ion *et al.* [61]	2015	231	security experts	12%
		294	general public	10%
Ur *et al.* [125]	2015	49	general public	4%
Butler and Butler [25]	2015	737	general public	6%
Wash *et al.* [131]	2017	134	students	19%
Pew Research [101]	2017	1040	Americans	12%
Renaud and Zimmermann [106]	2019	1095	students	10%

Table 2. Password Manager Encouraging & Deterring Factors (F*i*)

#	Encouraging Adoption	#	Deterring Adoption
F1	descriptive norms [8]	F1’	not wanting to be first [8]; influence of old patterns [62]
F2	perceived usefulness [8, 84, 12]	F2’	happy with existing solution [8, 11, 39] lack of control [8]
F3	experience of being hacked [8]		
F4	convenience [8, 39]	F4’	lack of time [11, 39]; learning cost [39]; setup cost [39, 21, 12]; wanting to master password management [8, 39]
F5	perceived ease of use [8, 84]	F5’	usability concerns [39, 87, 28, 30]; compatibility concerns [62]
F6	perceived vulnerability [8, 39, 11]	F6’	low risk perception [11]
F7	response efficacy [8, 39, 12, 84]	F7’	security and privacy concerns [8, 11, 84, 62]
F12	facilitating conditions [84]	F8’	low self efficacy [11]
F13	social need [8]	F9’	procrastination [11]
F14	subjective norms [8]	F10’	lack of information/uncertainty [11, 8, 109]
F15	fear [12]	F11’	monetary cost [8, 84]

Table 3. Example Participant Quotes

Factor	Quotes
Relative Usefulness	"*...I cannot remember what asks for what because some of them want a capital letter they want an @symbol they want a monkey you know you've no idea what they want so I cannot remember what rules apply to what website so it's a great advantage cos I can just whip it and do it and it means if I'm on an unfamiliar computer I've got all my passwords on my phone, so I can just have a quick look and go ...*" P2
Perceived Risk	"*I don't trust these services. just trust myself more than I trust an external service basically*" P25
Response Cost	"*it is difficult to remember them all because it keeps telling you to change them for security things sometimes you just can't remember what they are, you know*", P26

Table 4. Push, Pull and Mooring factors (F*i* refers to encouraging factors in Table 2, with F*i*' referring to the corresponding deterring factor)

	Pull Factors		Push Factors		Mooring Factors
F2	Relative usefulness* (29)	F4	Password management cost (dissatisfaction)* (14)	F6'	Perceived risk in general* (26)
F7	Response efficacy* (13)	F6	Perceived vulnerability (dissatisfaction)* (9)	F7'	Concern about security risks* (23)
F5	*Perceived ease of use (5)*	F2'	*No need (no dissatisfaction) (4)*	F7'	Concern about privacy risks (10)
	Control Factors			F4'	Learning cost (9)
F1	Descriptive norms* (19)			F4'	Set-up cost* (7)
	Innovativeness (5)			F11'	Financial cost* (6)
	Decision support (4)			F7'	*Concern about access risk* (5)*
F14	*Subjective norms* (3)*				*Phone device related problems (5)*
F10'	*Lack of information (3)*			F4'	*Concerns about efficiency (2)*

*The number in parentheses represents the number of times each factor was mentioned. Starred factors confirm those highlighted by Pearman *et al.* [99]. Italicised factors were excluded from the model due to their low numbers.

Table 5. Descriptive Data (number(percentage))

Gender	PM Usage	Age
Male:128(64%) Female: 68(34%)	Using:3(1%) Not Using:195(99%)	18-25:87(43%); 26-35:53(26%);36-45:37(18%) 46-55:16(8%);56+ 4(2%); Not provided:1(.5%)
Education		
Less than a high school diploma 18(9%); High school degree or equivalent 32 (16%); Some college, no degree 40 (20%); Associate degree 12(6%); Bachelor's degree 48(24%); Master's degree 30(15%); Professional 9 (4%); Doctorate 7(3%); Other 2(1%)		

Table 6. Descriptive Statistics

Hi	Construct	Min	Max	Mean	Std. Dev	Skewness	Kurtosis
H1	**Relative usefulness (RU)**	1.25	7.00	4.6073	1.16262	-.086	-.343
H2	**Response efficacy (PWMREFF)**	2.67	7.00	5.0488	1.08592	-.104	-1.104
H3	**Dissatisfaction (DISSAT)**	1.33	6.67	4.1380	1.00311	.062	-.287
H3.a	**Perceived vulnerability (PVUL)**	2.25	6.50	4.7247	.96742	-.170	-.537
H3.b	**Response cost (RCMAN)**	1.25	7.00	4.7828	1.09402	-.146	-.310
H4	**Perceived risk (PRISK)**	1.00	7.00	4.8283	1.51016	-.189	-1.272
H4.a	**Security concerns (PWMSEC)**	1.00	6.75	4.4874	1.38124	-.411	-.782
H4.b	**Privacy concerns (PWMPRIV)**	1.33	7.00	4.9226	1.17966	-.186	-.577
H5	**Learning cost (PWMLC)**	1.00	6.67	3.9764	1.26362	.017	-.752
H6	**Set-up cost (PWMSETC)**	1.67	7.00	4.6330	1.55115	-.033	-1.432
H7	**Monetary cost (PWMFEE)**	1.33	6.67	4.6633	1.21050	-.819	.191
H8	**Descriptive norm (DNORM)**	1.00	6.00	2.0909	1.52536	1.157	-.088
H9	**Intention (INT)**	3.00	7.00	5.0606	1.25386	.005	-1.235
	Exposure to hacking (HACK)	.00	6.50	1.1667	1.78189	1.607	1.734
	Innovativeness (INNOV)	1.67	7.00	4.7744	1.28054	-.219	-.802

Table 7. Variance Inflation Factor (Dependent Variable: Z score(INT))

	Collinearity Statistics			Collinearity Statistics	
Construct	**Tolerance**	**VIF**	**Construct**	**Tolerance**	**VIF**
H1: Relative usefulness	.410	2.437	**H2: Response efficacy**	.413	2.420
H3: Dissatisfaction	.482	2.076	**H4: Perceived risk**	.200	5.011
H3.a: Perceived vulnerability	.832	1.201	**H4.a: Security concerns**	.474	2.108
H3.b: Response cost	.663	1.508	**H4.b: Privacy concerns**	.437	2.290
H5: Learning cost	.353	2.833	**H6: Set-up cost**	.283	3.536
H7: Monetary cost	.750	1.334	**H8: Descriptive norm**	.461	2.167
Innovativeness	.489	2.043	**Exposure to hacking**	.735	1.361

Table 8. Average Variance Extracted for Validity Testing

Construct	AVE (>0.5)	Construct	AVE (>0.5)	Construct	AVE (>0.5)
H1: Relative usefulness	0.721	**H2: Response efficacy**	0.783		
H3: Dissatisfaction	0.779	**H3.a: Perceived vulnerability**	0.722	**H3.b: Response cost**	0.745
H4: Perceived risk	0.885	**H4.a: Security concerns**	0.702	**H4.b: Privacy concerns**	0.780
H5: Learning cost	0.694	**H6: Set-up cost**	0.861	**H7: Monetary cost**	0.809
H8: Descriptive norm	0.901	**H9: Intention**	0.823		
Innovativeness	0.834	**Exposure to hacking**	0.557		

Table 9. Construct Reliability (CA=Cronbach's Alpha)

Construct	#	CA	Construct	#	CA	Construct	#	CA
H1: Relative usefulness	4	.910	**H2: Response efficacy**	3	.914			
H3: Dissatisfaction	3	.913	**H3.a: Perceived vulnerability**	4	.910	**H3.b: Response cost**	4	.921
H4: Perceived risk	3	.958	**H4.a: Security concerns**	4	.904	**H4b: Privacy concerns**	3	.914
H5: Learning cost	3	.871	**H6: Set-up cost**	3	.949	**H7: Monetary cost**	3	.926
H8: Descriptive norm	4	.973	**H9: Intention**	3	.933			
Innovativeness	3	.937	**Exposure to hacking**	2	.703			

Table 10.

Model Fit		Model Comparison		
X2/df	**RMSEA**	**IFI**	**TLI**	**CFI**
Acceptable scale for good adequate fit				
<=2	<.06 **	>=.90	>=.90	>=.90
Recommended for further analysis				
>2	>.08	<.90	<.90	<.90

Fit Indices	Overall Measurement Model
X2 /df	1.136
RMSEA	.026
IFI	.985
TLI	.983
CFI	.985

***Left: Model Fit Indices Cut-off Values (Source: [57, 26]) **(Reasonable fit up to .08) Right: Summary of Overall Measurement Model**

Table 11. Structural Equation Model Results (*p<.001, **p<.005, *p<.05)**

	Independent Variables	Intention	Adoption	Risk	Dissatisfaction
H1	**Relative usefulness**	.178***(4.321)			
H2	**Response efficacy**	.140***(3.355)			
H3	**Dissatisfaction**	.076*(2.077)			
H3.a	**Perceived vulnerability**				.202***(3.193)
H3.b	**Response cost**				.229***(3.492)
H4	**Perceived risk**	-.182***(-3.584)			
H4.a	**Security concerns**			.981***(9.567)	
H4.b	**Privacy concerns**			.371***(6.030)	
H5	**Learning cost**	-.021(-.463)			
H6	**Set-up cost**	-.373***(-7.515)			
H7	**Monetary cost**	.010(.314)			
H8	**Descriptive norm**	.105**(2.727)			
H9	**Intention**		.626***(9.343)		
Control Variables					
	Innovativeness	.082*(2.192)			
	Age	.021(.733)			
	Gender	-.027(-.941)			
	Exposure to hacking				.261***(4.096)
	Number of passwords				.075(1.219)
Model Fit					
X^2/df= 1.557, IFI= .990, TLI= .948, CFI= .989, RMSEA= .053					