Determining key factors that lead to the adoption of password managers

Raymond Maclean
Jacques Ophoff

Determining key factors that lead to the adoption of password managers

Raymond Maclean and Jacques Ophoff
Department of Information Systems
University of Cape Town
Cape Town, South Africa
MCLRAY002@myuct.ac.za, jacques.ophoff@uct.ac.za

Abstract— **Passwords form part of our daily routine and even though there are alternative authentication mechanisms, such as biometrics, passwords stubbornly persist. Passwords have been around for the last few decades, but also the various problems associated with users trying to create passwords that are strong and secure. Users are faced with a cognitive burden in managing passwords which often leads to poor password practices or users recycling passwords across various accounts. While there is no anticipated end to the use of passwords, scholars have identified that passwords need to be better supported – one such method is using a password manager. There is a wealth of technical research relating to password managers, which has led to drastic improvements and the maturing of the technology. However, there is a little research on why people would choose to adopt password managers. To explore these factors, this research uses an adapted version of the Unified Theory of Acceptance and Use of Technology (UTAUT2) that includes trust as an additional construct. Using empirical data, the results of the study show that performance expectancy, habit, and trust are key factors in the intention to adopt a password manager.**

Keywords—technology adoption, password manager, information security, trust, UTAUT2, PLS-SEM.

I. INTRODUCTION

Passwords are used daily by almost every person to access a multitude of accounts, systems and websites. Initially, people only had a few passwords to remember, but with the growth of technology, the sheer volume of accounts with corresponding passwords has increased to the point where keeping track of each password is a burden. With cyber-crime on the rise, the requirements for creating a secure password for each system further complicates the problem, especially as people are reusing or recycling passwords.

While there have been attempts to replace passwords and alternative authentication methods, passwords stubbornly persist. While there is no single solution to the problem, one recommendation is to better support the use of passwords. One such method is using password managers, while they have been around for quite some time and are recommended by security experts, there still seems to be little uptake to using a password manager. While there is research into the various types of password managers, proposals, security concerns and recommendations, there is very little research on why some people adopt password managers. This paper intends to determine the key factors; therefore this paper will not address any technical security concerns of the tools.

The remainder of this paper is organised as follows. First, the problem behind passwords will be presented, this section includes password security, defining password managers, outlining the various available types and related work in the field. Next, the theoretical framework is discussed, this includes the hypotheses and conceptual model. The following chapter will address the research methodology that was used. This is followed by a section on data analysis and a discussion of the results. Lastly, the conclusion summarises the research contributions.

II. BACKGROUND

In the following subsections, some context around passwords, password problems and an outline of password managers is presented.

A. Password paradigm

Passwords are an integral part of every person's life; they are used daily to access a plethora of online services, systems, devices and computers. As these services have exponentially expanded over the last few decades, the number of login credentials and passwords that users need to recall has drastically increased. Although the death of passwords has been predicted by various key figures, security managers and corporate companies over the last two decades [1]–[4], passwords persist and will most likely remain for quite some time. The persistence of passwords has been acknowledged and irrespective of the ongoing attempt to replace passwords with a worldwide longing to have them replaced, they remain part of our daily lives [5]. It has been argued that no single solution or "silver bullet" would be the answer to the problem, but rather that, a "best-fit" solution would need to be adopted and as passwords would endure for the foreseeable future [5]. A recent report from Cybersecurity Ventures envisions that the "total universe of passwords will likely grow from approximately 90 billion today to 300 billion by 2020" [6, p. 2]. With an understanding of the password epitome, the next section will address password security.

B. Password security

Research into password security related problems dates back to 1979 [7]; this has allowed scholars to contribute a wealth of research in the field over the last few decades. Researchers conducted a systematic literature review that found there has not been a paradigm change in password management for over thirty-five years [8]. The security of passwords remains a significant problem with varying requirements for creating secure passwords, such as password length, alphanumeric characters, special characters and the use of passphrases.

Research into the "characteristics of over 6 million passwords" specifically looked into "password length, password composition, and password selection" [9, p. 130].

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

Further research into the composition of passwords set out by authentication designers indicated that passwords should not contain any username details, advising that they need to be several characters long and consist of uppercase, lowercase digits and special characters [10]. Gray, Franqueira and Yu [11] found four factors that influenced the recollection of secure passwords, further adding to the dilemma of password security. The requirements for complex passwords and the need to recall passwords places an increase in the cognitive demand of users to have secure passwords for each login. The quality of passwords is exceptionally lacking, with users often recycling passwords and struggling to recall their passwords [12]. More recent research found that people would re-use both complex and repeated passwords at a rate of "1.7" to "3.4" passwords across a spectrum of websites [13, p. 175]. Considering the password paradigm outlined in the previous section, and the challenges faced with password security, there is motivation "to better support the use of passwords" [5, p. 8], one method being the use of password managers.

C. *Password managers defined*

Password managers are "programs used to generate, encrypt, and store passwords for a client-side user" [14, p. 18]. Password managers make use of a master password to unlock a database of more complex passwords, decreasing the "cognitive burden" of users [15], [16]. It is accepted that "Password managers remove the effort from password management" [17, p. 1]. A password manager starts with the user and a master password. The master password unlocks the password manager system, allowing the user to access the secure database and functions of the password manager. Password managers add the benefit of only needing to recall a single secure master password, while the more complex or system generated passwords are stored securely. The password manager can then interact with the various login pages to either auto login or pass the account details to the required system.

D. *Types of password managers*

Password managers now encompass a comprehensive range of password manager schemes across a broad platform of devices, operating systems and technologies that cover client-side programs and mobile apps to cloud-based solutions. Password managers are available as open-source or closed-source packages. Three categories of password managers have been clarified: "desktop manager, online manager and portable manager" [18, p. 234], but there are some password managers that were provided by vendors of browsers, third parties and network-based "where passwords are backed up to the cloud and synced across the user's devices" [19, p. 449]. There is a wide selection of password managers, some noteworthy mentions from previous research [14] include: Encryptr, Passbolt and LastPass for online and cloud-based password managers. For mobile devices, there is a broad selection of mobile apps such as 1Password, Dashlane, KeePassMobile, iCloud Keychain, LastPass, mSecure, OpenIntents Safe for Android, PadLock and Roboform2Go. Client-side password managers include HandyPassword, KeePass2, Padlock, Password Safe and RoboForm to name a few. There is also the availability of browser-based plugins: Password Maker, Password Multiplier and PwdHash. For script-based password managers, there is the option of Password Composer while Password Generator is a considered as a bookmarklet based password manager.

E. *Related work*

Alkaldi and Renaud [20] researched the adoption and rejection of smartphone security tools in 2016; the tools included screen locking functionality, anti-malware applications and password managers, they concluded that smartphone users were not using the available security tools. The authors wanted to "model security behaviours in order to understand adoption or rejection of these tools", their adopted model showed "a number of important factors informing smartphone security intentions" but needed further work to "validate the model with Smartphone owners"[17, p. 142].

Later research then focused on the adoption and rejection of smartphone password managers using "reviews from application stores representing the opinions of users who chose to trial password managers" [17, p. 2]. Various factors that impacted adoption and rejection were found through an online survey with 352 respondents about "password manager use and exploring factors that encourage or discourage password manager adoption" [17, p. 3].

More recent research in 2017 investigated user's considerations in the adoption of password managers through an online survey that encompassed 248 paid participants [21]. The newer research also focused on the examination of forty-five emotions felt by users when using password managers "since emotion has been identified by work in psychology and communications as influential in other risk-laden decision-making" [21, p. 1]. The results of the study found that "convenience" and "usefulness" were part of the main factors leading to the adoption of password managers while security concerns were cited by users that did not use the tool [21, p. 1]. The authors also noted that the "purpose of such tools is often misunderstood by both "users" and "non-users" [21, p. 15]. The analysis of the emotions indicated that users of password managers were "likely to feel secure, admiring and energetic, and less likely to feel suspicious when using their password manager to log into a website" [21, p. 15].

III. Theoretical Framework

There are a broad variety of models and theories that cover individual acceptance of technology. The Unified Theory of Acceptance and Use of Technology (UTAUT) was created when researchers empirically compared eight user acceptance models in early 2003 [22]. "UTAUT has served as a baseline model and has been applied to the study of a variety of technologies in both organizational and non-organizational settings" [23, p. 158]. The model has key constructs that are linked to use behaviour. The original UTAUT model was further extended in 2012 to a second-generation model named UTAUT2 to address the consumer acceptance and use of Information Technology [23].

A revised UTUAT model based on "trust and acceptance of cloud computing" was used in which the author determined that "trust establishment was the main barriers to adopt cloud services and applications" [24, p. 133]. It can be argued that trust of cloud-based password managers would also influence the adoption of password managers. Trust was a clear underlying theme for participants in research conducted by Alkaldi and Renaud [17]. Trust is supported by Karole, Saxena and Christin [18] who found that users need a certain level of trust in third-parties when using an online password manager, while users were more likely to trust portable password managers given that they used on their own local devices which they had control over. In remote password storage "there is considerable trust in the third party since it holds all user passwords" [25, p. 320]. Trust of third-parties has been questioned, with the assumption that "the third-party cloud provider can be trusted" [26, p. 314], while more recent research conducted on the adoption of password managers by experts in computer security, found that trust also seemed to be an issue [27].

The researcher proposes an adapted version of the UTAUT2 model with "Trust" as an additional construct with a direct impact on "Behavioural Intention".

A. Hypotheses development and conceptual model

The research model will use an adapted version of the UTAUT2 model with the constructs that are outlined in the subsections below, for this study the various factors that moderate the relationship of each underlying construct will not be tested.

1) Performance Expectancy

Performance expectancy is "the degree to which an individual believes that using the system will help him or her to attain gains in job performance" [22, p. 447]. Performance expectancy affects behavioural intention.

- H1: Performance expectancy has a positive impact on the intention to adopt password managers.

2) Effort Expectancy

"Effort expectancy is defined as the degree of ease associated with the use of the system" [22]. Effect expectancy affects behavioural intention.

- H2: Effort expectancy has a positive effect on the intention to adopt password managers.

3) Social Influence

Social Influence is described as "the degree to which an individual perceives that important others believe he or she should use the new system" and the underlying construct has the "explicit or implicit notion that the individual's behavior is influenced by the way in which they believe others will view them as a result of having used the technology" [22, p. 451]. Social influence affects behavioural intention.

- H3: Social influence has a positive effect on the intention to adopt password managers.

4) Facilitating Conditions

"Facilitating conditions is the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system" [22, p. 453]. Facilitating conditions includes "aspects of the technological and/or organizational environment that are designed to remove barriers to use" [22, p. 453]. Facilitating conditions affects behavioural intention,

- H4: Facilitating conditions has a positive impact on the intention to adopt password managers.

5) Hedonic Motivation

Hedonic Motivation is defined as the "fun or pleasure derived from using a technology, and it has been shown to play an important role in determining technology acceptance and use" [23, p. 161]. It has a direct effect on behaviour intention.

- H5: Hedonic motivation has a positive impact on the intention to adopt password managers.

6) Price Value

Price Value can be described as the effect that "cost" and "pricing structure" influences the "consumers" use of technology were they comprehend the advantages against the cost of the technology [23, p. 161]. Price value affects behavioural intention.

- H6: Price value has a positive impact on the intention to adopt password managers.

7) Habit

"Habit has been defined as the extent to which people tend to perform behaviors automatically because of learning" [23, p. 162]. Habit affects behavioural intention.

- H7: Habit has a positive impact on the intention to adopt password managers.

8) Trust

Trust is defined as "the belief that you can trust someone or something" and that there is a perceived level that "something is safe and reliable" [28]. Trust was proposed as an additional construct in an extended UTAUT model where it was observed that it had a direct effect on behaviour intention and that "trust establishment was the main barriers to adopt cloud services and applications" [24, p. 133].

- H8: Trust has a positive impact on the intention to adopt password managers.

Based on the above discussion the conceptual research model predicts several factors which influence the adoption of password managers.

IV. METHODOLOGY

Given the limited time constraint for the honours research project and the rate at which technology trends change, the timeframe of this research project will be cross-sectional, it will review data on password manager adoption factors using existing literature, along with an online survey to gather data from respondents on their adoption factors as it currently exists.

The target audience consisted of random participants in various fields in technology or IT companies, the main set of respondents predominantly consisted of a large set of students, along with a small subset of staff at a large South African university. Due to the risk of the possible low usage of password managers, the questionnaire also targeted non-users by gathering information about their perceived option on password managers and its anticipated use.

The questionnaire consisted of 31 questions that would take approximately five to ten minutes to complete. To ensure research validity and reliability, the wording for each question was based on the UTAUT/UTAUT2 questions [22], [23] and the work on the extended UTAUT model with the trust construct [24]. The questions were measured using a 7-

point Likert scale. Demographic questions were then asked, followed by questions on account usage and online behaviour based on the work of Fagan, Albayram, Khan and Buck [21]. The survey was published online using the Qualtrics platform. The questions were checked, and a dry run was conducted to check for any errors. The survey link was distributed through official mailing lists within the university, while external participants were emailed and asked to distribute the link to the survey.

V. Data analysis and results

A total of 265 responses were recorded in Qualtrics over a two-week period, 3 participants were under the age of 18 and had to be removed from the survey. 71 participants did not complete the survey, and the incomplete responses were removed from the dataset, leaving a total of 191 responses with data that was used for analysis.

A. *Demographic information*

The demographic information provided by the 191 participants that completed the survey included gender, age, level of education and level of computer proficiency. Most of the responses (52.88%) were male, closely followed by female respondents (43.46%), while 3.65% of participants preferred not to answer. Most of the participants (53.40%) are between the age of 18 to 25 years old, the second highest respondents (26.70%) were between 35 to 54 years old while there was a small group (18.32%) between the age of 26 to 34. Only 1.57% of participants were between 55 to 65 years, and there were no participants over the age of 65.

Most participants are very well educated with no participants having less than high school education, 32.46% had a 4-year college degree, while 26.53% of the participants had some college diploma. 23.56% of the participants followed closely with high school / General Educational Development (GED) while the remainder of respondents (10.99%) had a master's degree, 7.33% indicated a 2-year college degree, while 3.14% had a doctoral degree, only one respondent (0.52%) held a professional or medical degree.

Most of the participants (38.74%) are highly proficient in the use of computers with 27.75% being very highly skilled and 23.56% being above average. Only 9.42% of participants considered themselves as average users, and one respondent (0.52%) was recorded as being below average. A summary of the demographic information is provided in Table 1.

Table 1. Demographic data

Demographic	Metric	Percentage	Count
Gender	Male	52.88%	101
	Female	43.46%	83
	Prefer not to answer	3.66%	7
Age	18-25 years old	53.40%	102
	26-34 years old	18.32%	35
	35-54 years old	26.70%	51
	55-65 years old	1.57%	3
	65 years or older	0.00%	0
Level of education	Less than High School	0.00%	0
	High School / GED	23.56%	45
	Some College	21.99%	42
	2-year College Degree	7.33%	14
	4-year College Degree	32.46%	62
	Master's Degree	10.99%	21
	Doctoral Degree	3.14%	6
	Professional / Medical Degree (JD, MD)	0.52%	1
Level of computer proficiency	Very Low	0.00%	0
	Low	0.00%	0
	Below average	0.52%	1
	Average	9.42%	18
	Above average	23.56%	45
	High	38.74%	74
	Very high	27.75%	53

B. *Accounts and online behaviour*

Most participants spend a considerable amount on time online. 98.43% are online more than five times a week, 1.05% went online about four to five times a week, while only one respondent (0.52%) went online two to three times a week.

The participants were asked if they were ever aware of having an account hacked or compromised. 29.84% of the responses indicated that they were aware of an account being compromised, while 54.97% were not aware of being compromised or hacked and 15.18% were unsure. There is a probability that some participants may not be willing to admit that their accounts were compromised and opted not to answer truthfully.

The number of accounts for internet website or services was grouped into six categories. Most participants either have ten to twenty or fewer accounts (58.64%) while 12.04% had five or fewer accounts. 16.23% of participants have fifty or fewer accounts while only 24 respondents (12.57%) had more than fifty accounts. One respondent (0.52%), indicated that they had no accounts, this may be an error in the response, or a misunderstanding of the question, given that the survey was sent out via email to all participants, indicating that they should at least have access to one account.

For the account usage of participants, on an average week, 41.36% used five or fewer accounts, while 36.65% used ten and 17.80% of participants used twenty or fewer accounts per week. There was an extremely low number of respondents (2.62%) who used fifty or fewer accounts per week. Only one participant (0.52%) used the accounts more than fifty times a week while on the contrast, two participants (1.05%) used none of the accounts.

The survey showed that many of the participants did not have unique passwords or sometimes re-used the same password. 40.84% of the participants had several unique passwords, but sometimes reused the same password, 39.79% had few unique passwords and did not vary them across accounts while only 12 respondents (6.28%) had fifty or less unique passwords. Only 10.47% had a unique password for each account, and 2.62% of participants had one password that they used across each account. Password complexity is not considered, hence even though only 20 respondents used a different password for each account; they may still be low entropy passwords and easy to guess.

C. *Data analysis tool*

The researcher is using Partial Least Squares Structural Equation Modelling (PLS-SEM) for the research model. Partial Least Squares (PLS) is an alternative analysis method for Structural Equation Modelling (SEM) that is "particularly suited to situations in which constructs are measured by a very large number of indicators and where maximum likelihood covariance-based SEM tools reach their limit" [29, p. 283]. PLS-SEM is an algorithm that is often used in Information System (IS) research for measuring the relationship of constructs in model-based research using latent variables [30]. The researcher used a tool named SmartPLS (version 3.2.7) for the data analysis. SmartPLS is frequently used in model-based research to "estimate the path coefficients, which calculates the strength of the relationships between independent and dependent variables" [31, p. 62]. "Model estimation delivers empirical measures of the relationships between the indicators and the constructs (measurement models), as well as between the constructs (structural model)" [32, p. 131].

D. Model analysis

The data was imported into SmartPLS and the latent variables Performance Expectancy (PE), Effort Expectancy (EE) Social Influence (SI), Facilitating Conditions (FC), Hedonic Motivation (HM), Price Value (PV), Habit (H), Trust (T) and Behavioural Intention (BI) were added to the model. Before proceeding with the analysis of the results, the algorithm must be checked for convergence. The PLS algorithm was calculated using a maximum of three hundred iterations, the stop criterion changes were assessed in the interim results and showed that the algorithm converged in five iterations, well below the set threshold.

The calculation of the PLS algorithm for the initial model included the path coefficients for the inner model and the outer weights/loadings for the outer model; the results show that most the outer loadings are above the required threshold of 0.7 [32]. The outer loadings of the three indicators were below the 0.7 thresholds and subsequently removed before further analysis. Indicators should only be detached if the values of Composite Reliability and Average Variance Extracted (AVE) are amplified [32]. The indicators were removed, and the PLS algorithm was recalculated, the removal of one indicator increased the AVE of FC from 0.541 to 0.693, while the removal of the other two indicators increased the AVE of PV from 0.477 to 0.809. The three indicators were left out of the model for further reliability and validity testing.

Composite Reliability (CR) is used in SEM-PLS to measure the internal consistency reliability. Hair Jr et al [32] indicate that "this measure of reliability takes into account the different outer loadings of the indicator variables", the authors further advise that "reliability varies between 0 and 1" and that higher values will show "higher levels of reliability" [32, p. 136]. Values of 0.60 to 0.70 are tolerable, while values below 0.60 show "a lack of internal consistency reliability" [32, p. 137]. The CR for the model shows that all constructs pass the composite reliability check with values well above the 0.7 thresholds.

Convergent Validity (CV) is defined as "the closeness with which a measure relates to (or converges on) the construct that it is purported to measure" [33, p. 59]. One method of establishing the closeness of the measurements on the construct is using the AVE [32]. An AVE value of 0.50 or higher is desirable as it would typically allow the construct to explain "more than half of the variance of its indicator", while values less than 0.50 would likely indicate that "more variance remains in the error of the items than in the variance explained by the construct [32, p. 138]. The AVE extracted for the model shows that all constructs are above the 0.50 threshold.

Discriminant Validity (DV) is defined as "the degree to which the measures of different constructs differ from one another" [30, p. 19]. DV is often measured together with CV if constructs are linked [33]. DV can be measured using cross-loadings to check the correlation of the indicators outer loadings or using the Fornell-Larcker criterion that compares "the square root of the AVE values with the latent variable correlations" [32, p. 139]. The performance of both methods was recently studied and found not to be entirely dependable in detecting problems with discriminant validity, as an alternative, Heterotrait-Monotrait ratio (HTMT) was nominated as a more accurate technique [32].

An HTMT report was generated for the model, a correlation close to 1 indicates a lack of DV, the acceptable threshold values for HTMT are 0.90 or if "constructs in the path model are conceptually more distinct" a more "conservative threshold value of 0.85" is proposed [32, p. 141]. H and BI loads at 0.877, below the threshold of 0.90, but very close, this could indicate a possible lack of discriminant validity. To truly assess the loading, the confidence interval of the HTMT can be obtained through a procedure known as bootstrapping. A bootstrap calculation was run on the model, the results of the calculation show the path coefficient for H and BI returning a value of 0.608 with a 97.50% level of confidence, indicating that the two constructs are empirically distant.

E. Hypothesis testing

The p-value is an indicator used by scholars to evaluate significance levels; it designates the likelihood of "erroneously rejecting a true null hypothesis" [32, p. 206]. If a researcher is accepting a significance level of 5%, the desired p-value must be lower than a value if 0.05 for the relationship to be regarded as significant at a 5% level, while for more rigours research scholars adopt a significance level of 1% which then requires a p-value of less than 0.01 to designate that the relationship is important [32]. The model was tested with a complete bootstrapping calculation using 5000 samples [32] to test the hypotheses. The results indicate that there are three hypotheses that are significant at a level of 1%, namely H1, H7 and H8, whereas the other hypotheses such as H2, H3, H4, H5 and H6 are not supported. Table 2 provides an overview of the findings.

Table 2. Overview of findings.

Hypothesis		Path Coefficient	t-Value	p-Value	Significance level	Outcome
H1	PE -> BI	0.326	5.430	0.000	p < .001	Supported
H2	EE -> BI	-0.019	0.354	0.723	-	Not supported
H3	SI -> BI	0.009	0.202	0.840	-	Not supported
H4	FC -> BI	-0.021	0.428	0.668	-	Not supported
H5	HM -> BI	-0.042	0.883	0.377	-	Not supported
H6	PV -> BI	0.056	1.271	0.204	-	Not supported
H7	H -> BI	0.517	10.409	0.000	p < .001	Supported
H8	T -> BI	0.162	3.736	0.000	p < .001	Supported

F. Summary of findings

The most substantial result of the significance test was that "Performance Expectancy", "Habit" and "Trust" have a positive impact on "Behavioural Intention" and the adoption of password managers. Trust strongly supports the additional construct that was proposed in the revised UTAUT model

[24] in section III. The significance test also indicated that "Effort Expectancy", "Social Influence", "Facilitating Conditions", "Hedonic Motivation" and "Price Value" were not regarded as having a positive relationship on "Behavioural Intention as originally theorised.

VI. Discussion

Based on the results of this study, three key factors that lead to the adoption of password managers were significantly supported.

A. Performance Expectancy

The participants in this study had a strong link to performance expectancy; finding password managers useful in their daily life while allowing them to accomplish things more quickly. Surprisingly, the use of password managers also increased the productivity amongst the participants. Convenience and usefulness were also identified in a study of user's consideration of password managers use [21]. Performance expectancy is a positive factor in the adoption of password managers.

B. Effort Expectancy

Participants in the study had a clear and understandable interaction with password managers. The data indicated that most of the participants found password managers easy to use or at least, easy to learn how to make use of password managers and become skillful in its intended use. Ease of use, learning and interaction does not seem to be a factor of password manager adoption, most likely since most users of password managers are very computer literate, well-educated and spend a considerable amount of time online.

C. Social Influence

Social influence seems to not play a role in the adoption factors; participants did not consider people that are important to them to influence their behaviour to start using password managers. Only a handful of participants would prefer to use password managers based on the value that they placed in the opinion of people that mattered to them; this was very closely offset by participants that somewhat to strongly disagreed. This shows that peers affecting the social influence of people are not a major driver in this study for the adoption of password managers.

D. Facilitating Conditions

Participants had the necessary resources and knowledge to use password managers; almost all of the respondents indicated that password managers are compatible with the other technologies that they use. There is also a strong indication that they can get help from others if difficulties arise when using password managers. It seems that users do not need any organisational or technical infrastructure to support the use of password managers.

E. Hedonic Motivation

Most of the participants were neutral when asked if they found password managers entertaining, fun or enjoyable. A small number somewhat agreed that password managers were fun, but more participants disagreed, while a higher number disagreed on the entertainment factor. Fun or pleasure in using password managers is not a strong factor in the adoption of the technology.

F. Price Value

The use of free password managers was very favourable amongst the participants; most people did not wish to pay for a password manager; if asked whether they were reasonably priced, most respondents were impartial. More participants, however, felt that password managers were good value for money and at the current price they offered good value. Given that there are many free and open source password managers, the cost and pricing do not seem to affect the adoption of password managers.

G. Habit

While there was a close correlation of the use of password managers becoming a habit for participants, more strongly disagreed. Many felt that they were not addicted to password managers and did not have to use them. The habit of using password managers to generate and store more secure passwords for sensitive accounts was more predominant with expert users [27]. The results of indicate that habit influences the use of password managers and that with more frequent use, habit will automatically become a part of using password managers.

H. Trust

Trust is a strong indicator with most of the participants; they felt that password managers are trustworthy and that they would adopt password managers if good encryption practices were used, especially with regular and secure backups of the password database. The option of an auditing system or environment also had a very positive impact, along with the good reputation of the password manager. The establishment of trust has a positive impact on the adoption of password managers [21].

Performance expectancy, habit and trust influence the use and adoption of password managers. Most participants indicated their intention to continue using password managers into the future and always try to use the technology daily on a more frequent basis.

VII. Conclusion

While there is a wealth of knowledge and prior research on password managers regarding prior shortcomings, various exploits and vulnerabilities, many of the research outcomes have provided insight into improvements and techniques to safeguard the underlying encrypted databases and systems. Research has shown that irrespective of the drive to replace passwords with other authentication methods, passwords stubbornly remain a part of daily life. The password paradigm shows no signs of slowing down, with the number of user accounts and passwords growing exponentially. Literature has indicated that users persist in using poor password practices and that the cognitive load placed on users to create secure passwords for each account led to recycling passwords across accounts.

Password managers have evolved since they were first conceptualised and matured to a point where they are very well suited to allow users to better support the use of passwords, yet little research has been conducted in the field on the adoption of password managers. This study examined the key factors that lead to the adoption of password managers and used an adapted UTAUT2 model as the theoretical framework. While suited to predict the factors that lead to the adoption and use of technology, the results of the model seem to indicate that only three key constructs had a positive effect on the behavioural intention for adopting password managers.

Performance expectancy was identified as having a positive effect on password manager adoption with data showing a perception that password managers were beneficial and improved efficiency. A second factor was habit and that the continual use of password managers will lead to enforcing the habit of creating more secure and unique passwords for each sensitive account. Trust, linked closely to reputation, was the third and major factor that influenced the intention to adopt password managers, especially if the password manager has good encryption with regular and secure backup options.

Acknowledgment

This work is based on the research supported wholly / in part by the National Research Foundation of South Africa (Grant Numbers 114838).

References

[1] M. Kotadia, "Gates predicts death of the password," *Security*, 2004. [Online]. Available: https://www.cnet.com/news/gates-predicts-death-of-the-password/.

[2] IBM, "IBM News room - 2011-12-19 IBM Reveals five innovations that will change our lives within five years - United States," 2011. [Online]. Available: https://www-03.ibm.com/press/us/en/pressrelease/36290.wss. [Accessed: 17-Mar-2018].

[3] D. Terdiman, "Google security exec: 'Passwords are dead,'" *Security*, 2013. [Online]. Available: https://www.cnet.com/news/google-security-exec-passwords-are-dead/.

[4] S. St Louis, "From security to cloud to AI and IoT: Visionaries from Citrix offer predictions for 2018 | Citrix Blogs," 2017. [Online]. Available: https://www.citrix.com/blogs/2017/11/09/from-security-to-cloud-to-ai-and-iot-visionaries-from-citrix-offer-predictions-for-2018/. [Accessed: 17-Mar-2018].

[5] C. Herley and P. Van Oorschot, "A research agenda acknowledging the persistence of passwords," *IEEE Secur. Priv.*, vol. 10, no. 1, pp. 28–36, 2012.

[6] S. Morgan and J. Carson, "The world will need to protect 300 billion passwords by 2020," 2017.

[7] R. Morris and K. Thompson, "Password security: a case history," *Commun. ACM*, vol. 22, no. 11, pp. 594–597, Nov. 1979.

[8] V. Taneski, M. Hericko, and B. Brumen, "Password security - No change in 35 years?," in *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2014 - Proceedings*, 2014, pp. 1360–1365.

[9] C. Shen, T. Yu, H. Xu, G. Yang, and X. Guan, "User practice in password security: An empirical study of real-life passwords in the wild," *Comput. Secur.*, vol. 61, pp. 130–141, 2016.

[10] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in *Proceedings of 2014 Network and Distributed System Security Symposium*, 2014.

[11] J. Gray, V. N. L. Franqueira, and Y. Yu, "Forensically-sound analysis of security risks of using local password managers," in *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*, 2016, vol. 5, pp. 114–121.

[12] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web - WWW '07*, 2007, p. 657.

[13] R. Wash, E. Rader, R. Berman, and Z. Wellmer, "Understanding password choices : How frequently entered passwords are re-used across websites," *Proc. Twelfth Symp. Usable Priv. Secur. (SOUPS 2016)*, no. Soups, pp. 175–188, 2016.

[14] C. Luevanos, J. Elizarraras, K. Hirschi, and J. Yeh, "Analysis on the security and use of password managers," in *2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT)*, 2017, pp. 17–24.

[15] Z. Li, W. He, D. Akhawe, and D. Song, "The emperor's new password manager: security analysis of web-based password managers," *23rd USENIX Secur. Symp. (USENIX Secur. 14)*, pp. 465–479, 2014.

[16] L. Zhang-Kennedy, S. Chiasson, and P. Van Oorschot, "Revisiting password rules: Facilitating human management of passwords," in *eCrime Researchers Summit, eCrime*, 2016, vol. 2016–June, pp. 81–90.

[17] N. Alkaldi and K. Renaud, "Why do people adopt, or reject, smartphone password managers?," *Eur. Work. Usable Secur.*, p. 15, 2016.

[18] A. Karole, N. Saxena, and N. Christin, "A comparative usability evaluation of traditional password managers," *Int. Conf. Inf. Secur. Cryptol.*, vol. ICISC 2010, pp. 233–251, 2010.

[19] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, "Password managers: Attacks and defenses," in *Proceedings of the 23rd USENIX Security Symposium*, 2014, pp. 449--464.

[20] N. Alkaldi and K. Renaud, "Why do people adopt, or reject, smartphone security tools?," *Proc. Tenth Int. Symp. Hum. Asp. Inf. Secur. Assur. (HAISA 2016)*, no. Haisa, pp. 135–144, 2016.

[21] M. Fagan, Y. Albayram, M. M. H. Khan, and R. Buck, "An investigation into users' considerations towards using password managers," *Human-centric Comput. Inf. Sci.*, vol. 7, no. 1, pp. 1–20, 2017.

[22] V. Venkatesh, M. G. Morris, G. B. Davis, F. D. Davis, R. H. Smith, and S. M. Walton, "User acceptance of information technology: toward a unified view," *MIS Q.*, vol. 27, no. 3, pp. 425–478, 2003.

[23] V. Venkatesh, J. Y. L. Thong, and X. Xu, "Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology," *MIS Q.*, vol. 36, no. 1, pp. 157–178, 2012.

[24] S. T. Alharbi, "Trust and acceptance of cloud computing: A revised UTAUT model," in *Proceedings - 2014 International Conference on Computational Science and Computational Intelligence, CSCI 2014*, 2014, vol. 2, pp. 131–134.

[25] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh, "Kamouflage: Loss-resistant password management," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6345 LNCS, pp. 286–302.

[26] L. Wang, Y. Li, and K. Sun, "Amnesia: A bilateral generative password manager," in *2016 IEEE 36th International Conference on Distributed Computing Systems*, 2016, vol. 2016–Augus, pp. 313–322.

[27] E. Stobert and R. Biddle, "Expert password management," in *Lecture Notes in Computer Science*, 2016, vol. 9551, pp. 3–20.

[28] Cambridge Dictionary, "Meaning of trust in the Cambridge english dictionary," 2018. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/trust. [Accessed: 26-Apr-2018].

[29] M. Haenlein and A. M. Kaplan, "A beginner's guide to partial least squares analysis," *Underst. Stat.*, vol. 3, no. 4, pp. 283–297, 2004.

[30] N. Urbach and F. Ahlemann, "Structural equation modeling in information systems research using partial least square least squares," *Inf. Syst. Res.*, vol. 11, no. 2, pp. 5–40, 2010.

[31] R. Crossler and F. Bélanger, "An extended perspective on individual security behaviors," *ACM SIGMIS Database*, vol. 45, no. 4, pp. 51–71, Nov. 2014.

[32] J. F. Hair Jr, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A primer on partial least squares structural equation modeling (PLS-SEM)*. 2017.

[33] A. Bhattacherjee, *Social science research: Principles, methods, and practices*. Scholar Commons, 2012.