Journal of Information Security & Cybercrimes Research 2021; Volume 4 Issue (2), 148-158

Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

User Acceptance of Password Manager Software: Evidence from Australian Microbusinesses

Hassan Jamil[1*], Tanveer Zia[2], and Tahmid Nayeem[3]

[1]UNSW Institute for Cyber Security, UNSW-Canberra, Australia.
[2] Center of Cybercrimes and Digital forensics, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.
[3]School of Management and Marketing, Charles Sturt University, Albury, Australia.

Received 12 Oct. 2021; Accepted 15 Dec. 2021; Available Online 30 Dec. 2021.

Abstract

While text passwords are still a pervasive authentication tool, their inadequacies are well recognized. Poorly chosen and weak passwords are the main reason behind security breaches. Multiple authentication techniques such as biometric, token-based, and knowledge-based authentication have been developed to overcome data leaks. However, acceptance of these authenticating techniques is complicated, and users find them hard to use. Microbusinesses, defined as having less than two employees, usually have very limited resources including budget, information security expertise and updated computer systems to fulfil the security requirements. Many microbusiness owners use the same information technology as in the home but for more sophisticated commercial reasons. An effective and easy way for microbusinesses to add an extra protection layer to their systems and passwords is through the use of password managers. This paper examines the useability and ease of use of the password manager software. We extended the Technology Acceptance Model (TAM) and tested the mediating role of self-efficacy on TAM's relationship with computer security usage. A sample of 420 microbusiness owners was taken to test the relationships among the variables through an online web-based survey. The results confirmed that self-efficacy plays a vital role in the user acceptance of password managers and reported its mediating role between perceived ease of use, perceived usefulness, and computer security usage.

I. Introduction

Passwords have dictated the world of authentication for more than 50 years as a common form of e-authentication used by the government for accessing the services by individuals [9]. The existing layers of protection are either complex to use or too simple to be prone to hacks and therefore require something more secure and easy to adopt [42]. Globally, electronic services become vulnerable to data breaches, virus attacks, malware attacks, phishing attacks etc. Effective e-authentication builds user confidence in dealing electronically with government agencies and is vital for service delivery with extra security.

Keywords: Computer security usage, password manager software, technology acceptance model, self-efficacy.

Production and hosting by NAUSS

* Corresponding Author: Hassan Jamil
Email: h.jamil@adfa.edu.au
doi: 10.26735/KPOB8473

Cybercrime in Australia costs small businesses around US$300 million a year [1]. This does not include business and government costs, while cybercrime costs will grow by 15% a year globally [2]. To reduce cybercrime threats and gain consumer trust, organizations have developed a range of security measures and robust authentication techniques such as the use of multifactor authentication, password managers, biometrics verification [3] [4]. These security plans cover three areas the people, technology, and process. Though, such technological innovations are only as good as a company [5] and consumer practices [6].

On the contrary, hackers' motives have evolved around state-sponsored attacks and organized crime. They steal personal information, bank details, credit card numbers, tax returns etc. More importantly, in small organizations, people are more likely to risk unauthorized data leakages [7, 44]. Indeed, with the greater usage of sensory devices, even in smartphones, the use of biometric or two-factor authentication has become more convenient [8, 9]. Prior research has focused only on the technical side of authentication technologies. However, user acceptance and adequacy are still unclear and not aligned with the sturdy technologies [10, 45].

However, continuous technological changes threaten the existing business model while still providing innovative services opportunities [11, 43]. With advanced technologies and dynamic growth, consumer acceptance of these technologies depends on many factors, such as availability, convenience, consumer demand and but not limited to security features.

In the past few decades, there has been a significant amount of research on the Technology Acceptance Model (TAM) replication, expansion, and modification, proving TAM's central position in the information security literature [15]. Past researchers have focused on the moderators and the TAM model's antecedents [16, 17]. Also, numerous studies are available that focuses on the factors affecting users' intentions to adopt IS services such as e-government services, mobile banking, security software, and consumer smartphones [17-20]. Currently, limited research is available that emphasizes, present, or further extend the TAM model by including new variables and how the TAM construct will behave in the presence of new variables.

This paper attempts to determine the adoption of Password Manager Software (PMS) and further extended the TAM literature to test the mediating role of self-efficacy on the individual's computer security usage. We propose that the TAM model constructs; perceived ease of use (PEU) and perceived usefulness (PU) employs their effect through self-efficacy. More specifically, in this study, we intend to explore the following objectives:

i. To analyze the PU of PMS and its relationship with individuals' computer security usage
ii. To analyze the PEU of PMS and its relationship with computer security usage
iii. To test the mediating role of self-efficacy on the relationship between PU of PMS and computer security usage
iv. To test the mediating role of self-efficacy on the relationship between PEU of PMS and computer security usage

We have made two mediating models to address these points, as shown in Fig. 1 and 2. Fig. 1 shows the mediating role of self-efficacy on the relationship between PEU and computer security usage. Likewise, Fig. 2 depicts the mediation role of self-efficacy on the relationship of PU and computer security usage.

In the next section, we first review the TAM Literature and then the efficacy theory literature. The general mediation model is introduced under the related work section II. Followed by section II, research methodology is discussed in detail in section III, which provides detailed insights about the data collection process, and the mediation analysis are also discussed in the results section. Finally, we discussed and summarized the results in the last sections of the research paper.

II. Related Work

The TAM proposed by Davis [22] appeared to be a suitable model for analyzing users' behaviors towards accepting new technologies and safe computing practices. The TAM model was initially practised in the industrial and organizational sectors and was proven vital in different situations and settings [18, 23].

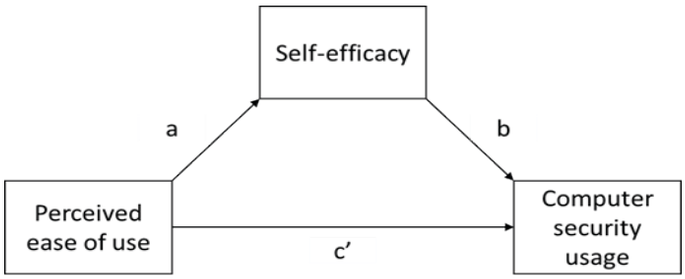

Fig. 1. Research model 1: mediation model for PEU.

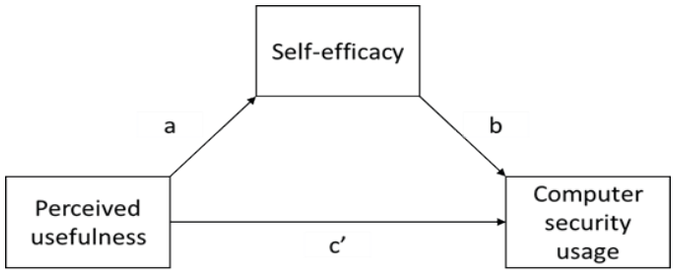

Fig. 2. Research model 2: mediation model for PU.

Where in the TAM, PEU is closely associated with PU. Moreover, regarding the adoption of technology and practices, both components of the TAM model, PU and PEU are important factors to consider. Herath, Chen [24] studied behaviors regarding the adoption of email authentication services by applying the combination of TAM, Technology Threat Avoidance Theory, and Protection Motivation Theory and found threat appraisal and coping appraisal both influence adoption.

Research by Piccolotto and Maller [25] on the use and acceptance of biometrics as an authentication tool and found that biometrics are useful. However, computer users still found them difficult to use. Conversely, password-protected security provides greater ease of use, but users were worried about the usefulness of passwords and showed their concerns as they are hard to remember. The usefulness of robust security protocols in cloud devices is important for protection and may provide greater user confidence; however, this may increase the system complexity [26].

Later, the Theory of Reasoned Action has been used in many behavioral types of research to explain users' intentions towards specific tasks [27]. Also, in the context of information security research, this construct has been further used in exploring individuals' behavioral intentions to adopt information technologies [28, 29].

TAM is also the most cited model in technology acceptance, consisting of two independent constructs: PEU and PU [22]. The PEU is the individuals' belief to use system/software as effortless, whereas PU is the user's perception that the specific system/technology would improve his/her job performance [19].

In addition to this, the TAM model was developed originally to explore the adoption of spreadsheet software and applied in other domains [27, 30, 31]. The TAM model has been used in past research as Piccolotto and Maller [25] have utilized it to find out the user acceptance of biometric devices and users' experience with these devices. It was found that password protection provides greater PEU but lower PU because complex passwords can easily be forgotten.

Efficacy Theory and TAM

The self-efficacy theory suggests that individuals' behavior, such as adopting the latest security-related technologies, is the outcome of efficacy appraisal, through which they examine the efficacy of performing a specific action [21, 32]. In addition,

if the individuals have prior knowledge to perform a recommended action, such as PMS installation and know the consequences of weak passwords, they will install it. In contrast, the efficacy appraisal concludes that if the individual does not have high efficacy, he will not engage himself/herself in a recommended behavior [33]. Further, it might be possible that these perceptions are affected by some exogenous variables such as PEU and PU.

Moreover, self-efficacy refers to individuals believing that he/she has sufficient knowledge and is aware of the adverse consequences if the recommended action has not been taken or adopted [15, 21, 32]. Polites and Karahanna [34] have tested the PEU and found its association with self-efficacy. Pavlou and Fygenson [35] have also tested self-efficacy and the PEU and found a significant relationship among them. In contrast, the PU would increase the user's self-confidence to adopt a recommended behaviour.

III. Methodology

A. Data collection and sampling plan

This research is based on the web-based online survey using Qualtrics, and the questionnaires were distributed via paid service from the panel provider. The online survey design allowed us to collect data from multiple participants from across Australia in an efficient manner.

The sampling frame was the Australian small business owners who do not employ more than two employees in their business. Further, some filter questions were included at the beginning of the survey, and many criteria had to be met to qualify for inclusion in the research. This survey only focused on users who have previously installed the PMS or currently have it and are over 18. We also excluded those businesses that employed more than two people in their businesses.

B. Measures

The survey questionnaire was adapted from prior researches, and the indicators have already been tested and validated. The measurement scale of PU and PEU was adapted from the study of Davis [22]. Further, the computer security usage variable scale was taken from the study of Claar and Johnson [36]. Lastly, the self-efficacy scale was adapted from the study of Johnston, Warkentin [37].

A complete questionnaire used in this survey can be seen in Appendix A.

C. Data Analysis and Results

The statistical analysis was performed using the IBM SPSS v26 software. The mediation analysis was performed through the process plugin developed by Hayes (2013). The sample descriptive information and the demographics can be seen in Table I. In addition to that, the Confirmatory Factor Analysis was performed, and reliability analysis was done to check the discriminant and convergent validity of the constructs.

D. Response Rate

A total number of 924 questionnaires were distributed for this research study, out of which 502 respondents were qualified to participate in the survey, as shown in Table II. In addition to that, 422 survey questionnaires were discarded as those respondents were failed to meet the selection criteria. After removing the outliers, only 420 survey questionnaires were found completed and included in the survey for the analysis.

E. Missing Values

The data was collected online through the Qualtrics software, and therefore, no skip logic was used to avoid the missing values. The data was screened for analysis, and none of the values was recorded missing.

F. Outliers

The data was further screened by analyzing the outliers in the given data in the SPSS software. Initially, the total number of qualified record-ed responses were 502 before removing the outliers. After performing the outlier analysis in the SPSS, 82 responses were detected as outliers and excluded from the survey.

TABLE I
DESCRIPTIVE STATISTICS OF THE SAMPLE POPULATION

		Frequency	Percentage	Valid Percent	Cumulative Percentage
Business Location	(New South Wales (NSW	133	26.5	26.5	26.5
	Victoria	143	28.5	28.5	55
	Queensland	100	19.9	19.9	74.9
	Western Australia	42	8.4	8.4	83.3
	South Australia	62	12.4	12.4	95.6
	Tasmania	15	3	3	98.6
	Australian Capital Territory	5	1	1	99.6
	Northern Territory	2	0.4	0.4	100
	Total	502	100	100	
Gender	Male	286	57	57	57
	Female	216	43	43	100
	Total	502	100	100	
Age	24 - 18	5	1	1	1
	34 - 25	37	7.4	7.4	8.4
	44 - 35	70	13.9	13.9	22.3
	54 - 45	105	20.9	20.9	43.2
	64 - 55	144	28.7	28.7	71.9
	74 - 65	119	23.7	23.7	95.6
	84 - 75	20	4	4	99.6
	or older 85	2	0.4	0.4	100
	Total	502	100	100	
Education	Went to high school but did not finish year 10	15	3	3	3
	Year 10	22	4.4	4.4	7.4
	Year 11	20	4	4	11.4
	(Finished High School (year 12	105	20.9	20.9	32.3
	Some university	95	18.9	18.9	51.2
	Undergraduate degree	173	34.5	34.5	85.7
	Master's degree	57	11.4	11.4	97
	Doctorate	15	3	3	100
	Total	502	100	100	

TABLE II
SURVEY RESPONSE RATE

Surveys	Frequency	Percent
Distributed	924	100%
Returned	502	54.33%
Useable	420	45.67%

G. Confirmatory Factor Analysis

Table III represents the final factor scores along with the values of Average Variance Extracted (AVE) and the Composite Reliability (CR) values. The values of AVE should be above 0.5, and the CR for all constructs should be above 0.7 [38]. The variable measures for all items have shown discriminant validity. The AVE and the CR values fall within the acceptable range as described by Fornell and Larcker [38].

H. Mediation effect of self-efficacy on the relationship between PEU and computer security usage

Table IV represents the mediation effect of self-efficacy on the relationship between PEU and computer security usage. For PEU based model, bootstrapping results show the total effect of PEU on computer security usage (c path, total effect = 0.321, p = 0.000), which is significant and the direct effect of PEU on computer security usage (c' path, direct effect = 0.211, p = 0.000) which is also significant, a change in interaction values shows the direction of the relationship and further the self-efficacy partially mediates between the relationship of PEU and computer security usage. Therefore, we conclude that self-efficacy is mediating partially on the relationship between PEU and an individual's computer security usage.

TABLE III
CFA ANALYSIS RESULTS

			Estimate	AVE	CR
SE3	--->	self_eff	0.837		
SE2	--->	self_eff	0.861		
SE1	--->	self_eff	0.828	0.70	0.895
SCP1	--->	csu	0.810		
SCP2	--->	csu	0.758		
SCP3	--->	csu	0.861	0.651	0.850
PU4	--->	perc_usef	0.9		
PU5	--->	perc_usef	0.804		
PU6	--->	perc_usef	0.634		
PU3	--->	perc_usef	0.931		
PU2	--->	perc_usef	0.88		
PU1	--->	perc_usef	0.707	0.666	0.921
PEU4	--->	perc_eofu	0.725		
PEU5	--->	perc_eofu	0.776		
PEU6	--->	perc_eofu	0.831		
PEU3	--->	perc_eofu	0.843		
PEU2	--->	perc_eofu	0.818		
PEU1	--->	perc_eofu	0.842	0.651	0.917

TABLE IV
MEDIATION ANALYSIS FOR PEU

Mediation path analysis			
	Coeff.	**SE**	**t**
a Path	0.581	0.038	15.265***
b Path	0.190	0.086	2.206***
c Path	0.321	0.068	4.760***
c' Path	0.211	0.084	2.512***

Notes: a path= independent variable to the mediator; b path = mediator on dependent variable; c path = Total Effect Independent variable on dependent variable; c' path = Direct Effects independent variable on dependent variable; sample size 420, Number of Bootstrap Resamples = 5000; Furthermore, R^2 Y, X is the proportion of the variance in the dependent variable (DV) by the independent variable (IV) which was 0.062***. However, R^2 M, X is the proportion of the variance in a mediator (M) explained by independent (IV) which was 0.358***. R^2 Y, MX is the proportion of the variance in the dependent variable (DV) by a mediator (M) and independent variable (IV) together which was 0.051***.

TABLE V
MEDIATION ANALYSIS FOR PU

Mediation path analysis			
	Coeff.	**SE**	**t**
a Path	0.335	0.036	***9.218
b Path	0.179	0.075	***2.396
c Path	0.341	0.056	***6.109
c' Path	0.281	0.061	***4.616

Notes: a path= independent variable to the mediator; b path = mediator on dependent variable; c path = Total Effect Independent variable on dependent variable; c' path = Direct Effects independent variable on dependent variable; sample size 420, Number of Bootstrap Resamples = 5000; Furthermore, R^2 Y, X is the proportion of the variance in the dependent variable (DV) by the independent variable (IV) which was 0.094***. However, R^2 M, X is the proportion of the variance in a mediator (M) explained by independent (IV) which was 0.169***. R^2 Y, MX is the proportion of the variance in the dependent variable (DV) by a mediator (M) and independent variable (IV) together which was 0.082***.

I. Mediation effect of self-efficacy on the relationship between PU and computer security usage:

Table V represents the mediation effect of self-efficacy on the relationship between PU and computer security usage. For PU based model, bootstrapping results show the total effect of PU on computer security usage (c path, total effect = 0.341, p = 0.000), which is significant and the direct effect of PEU on computer security usage (c' path, direct effect = 0.281, p = 0.000) which is also significant, a change in interaction values shows the direction of the relationship and further the self-efficacy partially mediates between the relationship of PU and computer security usage. Therefore, we conclude that self-efficacy mediates partially on the relationship between PU and individual computer security usage.

IV. DISCUSSION

This study attempts to achieve the four objectives discussed in section I. The first two objectives assess the impact of PEU and PU of PMS on users' computer security usage. Table IV and Table V indicate that PEU and PU significantly impact the user's security usage. This means that if the users find PMS easy to use and useful, they are more likely to install and use it. These findings are consistent with the study of [39].

The third objective was to identify the mediating role of self-efficacy on the relationship between PEU and computer security usage. Table IV and Table V reveal that self-efficacy partially mediates the relationship between PEU and computer security usage. Moreover, the fourth objective was to discover the mediating role of self-efficacy between the relationship of PU and computer security usage. We found that self-efficacy partially mediated the relationship between PU and computer security usage. The slight change in the interaction values of total effects in both tables indicates the mediation relationship direction. This shows that higher individuals' self-efficacy is more likely to install PMS and adopt more secure technologies.

As discussed in sections 'H' &' I', the mediation results indicated that both PU and PEU significantly impact the user's security usage behaviors. The microbusiness owners perceive PMS as a vital tool for increasing their password security. Fagan, Albayram [40], Alodhyani, Theodorakopoulos [41] also indicates that users with high computer proficiency and better computer experience found password managers convenient, secure, and useful to increase their password security. The findings

of the study support Fagan, Albayram [40], and the results show microbusiness owners have sufficient computer knowledge and experience. These findings are interesting for cybersecurity practitioners and developers and provide them insights about the layperson's level of efficacy and literacy about computer applications. Further, they understand the importance of strong passwords and install PMS for its effectiveness.

V. Limitations and Future Research

The first limitation of the study was that we had applied this research to small businesses. However, future research can be done by testing this model for large organizations. Furthermore, replicating the mediating model in different industrial sectors will provide more insights towards understanding secure behaviors. We only focused on one part of the efficacy theory, including self-efficacy, and excluded the response efficacy. Further investigations can be done by including the response efficacy, which can provide better insights in understanding the efficacy variables and their effect on the TAM and user security adoption behaviors.

VI. Conclusion

The paper tested and provided evidence for the effect of self-efficacy on the useability and adoptability of the PMS. In particular, the study has managed to disclose that computer self-efficacy plays a vital role and influences individuals towards PMS acceptance. The findings validate the TAM theory, and the results also validate its application in information security research. The study reveals some important implications for practitioners and managers to consider self-efficacy as a significant factor that could help to promote the adoptability of the PM by the microbusiness's owners. Further, these findings also provide some important insights to the governments to encourage users towards password security management and initiate some awareness campaigns or training to increase the individual's computer software related efficacy. The results effectively answered the research objectives and identified the mediating role of self-efficacy with respect to technology acceptance.

The study provides empirical evidence for mediating the role of self-efficacy between the relationship or PEU and PU on an individual's actual usage behaviors rather than intentions. The outcomes of the survey revealed that individuals are more likely to install password managers when they have a better understanding of the security software and good efficacy.

We acknowledge that we focused on the general password manager software that is available easily to the users; however, more research is needed to identify any specific PMS adoptability. The predicted effects prove the microbusiness owner's adoption intentions and also the actual security usage. Further, the findings reveal strong evidence of the importance of self-efficacy with respect to technology acceptance.

References

[1] Australian Cyber Security Centre, “ACSC Threat Report 2015,” July 15, 2015. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-threat-report-2015

[2] S. Morgan, “Cybercrime To Cost The World $10.5 Trillion Annually By 2025,” Nov. 13, 2020. Accessed: Dec. 11, 2021. [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[3] T. Bui, and T. Aura, “GPASS: A password manager with group-based access control,” in *Nordic Conference on Secure IT Systems (NordSec 2017)*, in Secure IT Systems, H. Lipmaa, A. Mitrokotsa, and R. Matulevicius, Eds., in Lecture Notes in Computer Science, vol. 10674, 2017.

[4] K. Yeh, C. Su, W. Chiu and L. Zhou, "I Walk, Therefore I Am: Continuous User Authentication with Plantar Biometrics," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 150-157, Feb. 2018, doi: 10.1109/MCOM.2018.1700339.

[5] S. R. Boss, L. J. Kirsch, R. A. Shingler, and R. W. Boss, “If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security,” *Eur. J. Inf. Syst.*, vol. 18, p. 151-164, 2009, doi: 10.1057/ejis.2009.8.

[6] M. Whitty, J. Doodson, S. Creese, and D. Hodges, “Individual differences in cyber security behaviors: An examination of who is sharing passwords,” *CyberPsychol. Behav. Soc. Netw.*, vol. 18, no. 1, p. 3-7, Jan. 1, 2015, doi: 10.1089/cyber.2014.0179.

[7] P. Engle, “Cybersecurity basics,” *Ind. Eng.*, vol. 48, no. 1, Jan. 2016.

[8] V. Zimmermann and N. Gerber. ""If it wasn't secure, they would not use it in the movies"–security perceptions and user acceptance of authentication technologie," in *Int. Conf. Hum. Asp. Inf. Secur. Priv. Trust*, in Human Aspects of Information Security, Privacy and Trust, T. Tryfonas Ed., in Lecture Notes in Computer Science, vol 10292, 2017, doi: 10.1007/978-3-319-58460-7_18.

[9] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "Passwords and the evolution of imperfect authentication," *Commun. ACM*, vol. 58, no. 7, p. 78-87, July 2015, doi: 10.1145/2699390.

[10] R. R. Heckle, A. S. Patrick, and A. Ozok, "Perception and acceptance of fingerprint biometric technology," in *Proc. 3rd Symp. Usable Priv. Secur.*, Pittsburgh, PA, USA, July 18, 2007, p. 153-154, doi: 10.1145/1280680.1280704.

[11] P. C. Lai, "Design and Security impact on consumers' intention to use single platform E-payment," *Interdiscip. Inf. Sci.*, vol. 22, no. 1, p. 111-122, 2016, doi: 10.4036/iis.2016.R.05.

[12] P. C. Lai, "Security as an extension to TAM model: Consumers' intention to use a single platform e-payment," *Asia-Pac. J. Manag. Res. Innov.*, vol. 13, no. 3-4, p. 110-119, Sept. 2017, doi: 10.1177/2319510X18776405.

[13] P. Luarn and H.-H. Lin, "Toward an understanding of the behavioral intention to use mobile banking," *Comput. Hum. Behav.*, vol. 21, no. 6, p. 873-891, Nov. 2005, doi: 10.1016/j.chb.2004.03.003.

[14] X. Zhang, X. Han, Y. Dang, F. Meng, X. Guo, and J. Lin, "User acceptance of mobile health services from users' perspectives: The role of self-efficacy and response-efficacy in technology acceptance," *Inform. Health Soc. Care*, vol. 42, no. 2, p. 194-206, Aug. 26, 2016, doi: 10.1080/17538157.2016.1200053.

[15] Y. He, Q. Chen, and S. Kitkuakul, "Regulatory focus and technology acceptance: Perceived ease of use and usefulness as efficacy," *Cogent Bus. Manag.*, vol. 5, no. 1, p. 1-22, Apr. 2018, doi: 10.1080/23311975.2018.1459006.

[16] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Q.*, vol. 27, no. 3, p. 425-478, Sept. 2003, doi: 10.2307/30036540.

[17] Y.-M. Cheng, "Antecedents and consequences of e-learning acceptance," *Inf. Syst. J.*, vol. 21, no. 3, p. 269-299, Aug. 16, 2010, doi: 10.1111/j.1365-2575.2010.00356.x.

[18] F. Weng, R. JouYang, H. Ho and H. Su, "A Study of Elementary School Teachers' Intention to Use Multimedia Materials Based on the Technology Acceptance Model-A Case Study of Elementary Schools in Chiayi County," in *2017 Int. Conf. Inf. Commun. Eng. (ICICE)*, Xiamen, China, 2017, pp. 98-100, doi: 10.1109/ICICE.2017.8478890.

[19] L. G. Wallace and S. D. Sheetz, "The adoption of software measures: A technology acceptance model (TAM) perspective," *Inf. Manag.*, vol. 51, no. 2, p. 249-259, Mar. 2014, doi: 10.1016/j.im.2013.12.003.

[20] P. B. Lowry, T. Dinev, and R. Willison, "Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda," *Eur. J. Inf. Syst.*, vol. 26, no. 6, p. 546-563, Feb. 15, 2018, doi: 10.1057/s41303-017-0066-x.

[21] K. Witte, "Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures," in *Handbook of Communication and Emotion*, P.A. Andersen and L.K. Guerrero, Eds., San Diego, CA, USA: Academic Press, 1996, p. 423-450.

[22] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Q.*, vol. 13, no. 3, p. 319-340, 1989, doi: 10.2307/249008.

[23] J. Schepers and M. Wetzels, "A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects," *Inf. Manag.*, vol. 44, no. 1, p. 90-103, Jan. 2007, doi: 10.1016/j.im.2006.10.007.

[24] T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, and H. R. Rao, "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," *Inf. Syst. J.*, vol. 24, no. 1, p. 61-84, July 27, 2012, doi: 10.1111/j.1365-2575.2012.00420.x.

[25] P. Piccolotto and P. Maller, "Biometrics from the user point of view; Deriving design principlese from user perceptions and concerns about biometeric systems," *Intel Technol. J.*, vol. 18, no. 4, p. 30-44, 2014.

[26] S. Dey, S. Sampalli, and Q. YE, "Security and privacy issues in mobile cloud computing," *Int. J. Bus. Cyber Secur.*, vol. 1, no. 1, p. 31-43, July 2016.

[27] E. Karahanna, R. Agarwal, and C. M. Angst, "Reconceptualising compatibility beliefs in technology acceptance research," *MIS Q.*, vol. 30, no. 4, p. 781-804, 2006, doi: 10.2307/25148754.

[28] V. Assadi and K. Hassanein, "Continuance intention to use high maintenance information systems: The role of perceived maintenance effort," in *Proc. Eur. Conf. Inf. Syst. (ECIS 2010)*, Pretoria, South Africa, 2010, p. 94.

[29] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Comput. Secur.*, vol. 49, p. 177-191, Mar. 2015, doi; 10.1016/j.cose.2015.01.002.

[30] R. Hirschheim, "Introduction to the special issue on" quo vadis TAM-issues and reflections on technology acceptance research"," *J. Assoc. Inf. Syst.*, vol. 8, no. 4, p. 9, 2007, doi: 10.17705/1jais.00128.

[31] I. Benbasat and W. Wang, "Trust in and adoption of online recommendation agents," *J. Assoc. Inf. Syst.*, vol. 6, no. 3, p. 4, 2005, doi: 10.17705/1jais.00065.

[32] E. K. Maloney, M. K. Lapinski, and K. Witte, "Fear appeals and persuasion: A review and update of the extended parallel process model," *Soc. Personal. Psychol. Compass*, vol. 5, no. 4, p. 206-219, Apr. 3, 2011, doi: 10.1111/j.1751-9004.2011.00341.x.

[33] K. Maennel, R. Ottis, and O. Maennel. "Improving and measuring learning effectiveness at cyber defense exercises," in *Nordic Conference on Secure IT Systems*, in Secure IT Systems, H. Limpaa, A. Mitrokotsa, and R. Matulevicius, Eds., in Lecture Notes on Computer Science, vol. 10674, 2017, pp. 123-138.

[34] G. L. Polites and E. Karahanna, "Shackled to the Status Quo: The Inhibiting Effects of Incumbent System Habit, Switching Costs, and Inertia on New System Acceptance," *MIS Q.*, vol. 36, no. 1, p. 21-42, Mar. 2012, doi: 10.2307/41410404.

[35] P. M. Pavlou and M. Fygenson, "Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior," *MIS Q.*, vol. 30, no. 1, p. 115-143, Mar. 2006, doi: 10.2307/25148720.

[36] C. L. Chet and J. Johnson, "Analysing home PC security adoption behavior," *J. Comput. Inf. Syst.*, vol. 52, no. 4, p. 20-29, 2012, doi: 10.1080/08874417.2012.11645573.

[37] A. C. Johnston, M. Warkentin, and M. Siponen, "An enhanced fear appeal rehtorical framework: Leveraging threats to human asset through sanctioning rhetoric," *MIS Q.*, vol. 39, no. 1, p. 113-134, 2015, doi: 10.25300/MISQ/2015/39.1.06.

[38] C. Fornell and D.F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. Mark. Res.*, vol. 18, no. 1, p. 39-50, 1981, doi: 10.1177/002224378101800104.

[39] E. Stobert, T. Safaie, H. Molyneaux, M. Mannan, and A. Youssed, "ByPass: Reconsidering the usability of password managers," in *Int. Conf. Secur. Priv. Commun. Syst.*, in Security and Privacy in Communication Networks, N. Park, K. Sun, S. Foresti, K. Butler, and N. Saxena, Eds., in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 335, 2020, pp. 446-466.

[40] M. Fagan, Y. Albayram, M. M. Khan, and R. Buck, "An investigation into users' considerations towards using password managers," *Hum.-Centric Comput. Inf. Sci.*, vol. 7, no. 1, p. 1-20, 2017, doi: 10.1186/s13673-017-0093-6.

[41] F. Alodhyani, G. Theodorakopoulos, and P. Reinecke, "Password managers—It's all about trust and transparency," *Future Internet*, vol. 12, no. 11, p. 189, doi: 10.3390/fi12110189.

[42] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, "Why people (don't) use password managers effectively," in *Fifteenth Symp. Usable Priv. Secur.*, Santa Clara, CA, USA, Aug. 12-13, 2019, pp. 319-338.

[43] M. Hock-Doepgen, T. Clauss, S. Kraus, and C.-F. Cheng, "Knowledge management capabilities and organizational risk-taking for business model innovation in SMEs," *J. Bus. Res.*, vol. 130, pp. 683-697, June 2021, doi: 10.1016/j.jbusres.2019.12.001.

[44] R. Luna, "Stranger Danger!: How Hackers Break into School Databases to Steal Student Data, and What Legislatures Should Do about It," *SSRN Electr. J.*, Feb. 7, 2021, doi: 10.2139/ssrn.3781055.

[45] S. A. Kamal, M. Shafiq, and P. Kakria, "Investigating acceptance of telemedicine services through an extended technology acceptance model (TAM)," *Technol. Soc.*, vol. 60, Feb. 2020, doi: 10.1016/j.techsoc.2019.101212

Appndix

Appndix A

Research Questionnaire and Individual's Responses on 5-Point Likert Scale (N=420)

Items	Responses						
Self-efficacy	**Strongly Disagree (%)**	**Disagree (%)**	**Neutral (%)**	**Agree (%)**	**Strongly Agree (%)**	**Mean**	**Std Deviation**
Password manager software is easy to use.	0.01	0.03	0.52	0.32	0.14	2.46	0.81
Password manager software is convenient to use.	0.01	0.04	0.45	0.34	0.15	2.41	0.83
I am able to use a password manager without much effort.	0.02	0.07	0.45	0.28	0.16	2.51	0.86
Computer security usage	**Strongly Disagree (%)**	**Disagree (%)**	**Neutral (%)**	**Agree (%)**	**Strongly Agree (%)**	**Mean**	**Std Deviation**
I use add-on antivirus software on my computer(s)	0.05	0.07	0.11	0.25	0.51	1.89	1.16
I use add-on firewall software on my computer (s)	0.06	0.11	0.24	0.21	0.39	2.25	1.25
I use add-on anti-spyware software on my computer (s)	0.06	0.13	0.21	0.23	0.36	2.31	1.25
Perceived Usefulness	**Strongly Disagree (%)**	**Disagree (%)**	**Neutral (%)**	**Agree (%)**	**Strongly Agree (%)**	**Mean**	**Std Deviation**
Using password manager software in my job would enable me to accomplish tasks more quickly	0.06	0.14	0.48	0.21	0.1	2.84	1.01
Using password manager software would improve my job performance	0.12	0.17	0.46	0.18	0.08	3.02	1.05
Using password manager software in my job would increase my productivity	0.13	0.19	0.48	0.15	0.06	3.18	1.02
Using password manager software would enhance my effectiveness on the job.	0.13	0.17	0.44	0.19	0.07	3.09	1.07
Using password manager software would make it easier to do my job	0.14	0.18	0.41	0.21	0.07	3.09	1.11
I would find password manager software useful in my job.	0.12	0.18	0.33	0.25	0.12	2.93	1.17
Perceived ease of use	**Strongly Disagree (%)**	**Disagree (%)**	**Neutral (%)**	**Agree (%)**	**Strongly Agree (%)**	**Mean**	**Std Deviation**
Learning to operate password manager software would be easy for me	0.03	0.08	0.31	0.37	0.21	2.35	0.99
I would find easy to get password manager software to do what I want to do	0.03	0.07	0.37	0.36	0.16	2.45	0.96
My interaction with password manager software would be clear and understandable	0.02	0.07	0.37	0.37	0.16	2.41	0.91
I would find password manager software to be flexible to interact with	0.02	0.09	0.44	0.32	0.12	2.57	0.89
It would be easy for me to become skilful by using password manager software	0.02	0.07	0.32	0.41	0.19	2.33	0.93
I would find using password manager software easy to use.	0.02	0.06	0.31	0.41	0.22	2.29	0.91