Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 184 (2021) 266–274

Procedia Computer Science

www.elsevier.com/locate/procedia

The 12th International Conference on Ambient Systems, Networks and Technologies (ANT)
March 23-26, 2021, Warsaw, Poland

Understanding Dynamics of Initial Trust and its Antecedents in Password Managers Adoption Intention among Young Adults

Ali Farooq*, Alina Dubinina, Seppo Virtanen, Jouni Isoaho

Department of Computing, University of Turku,, Turku, Finland

Abstract

Security professionals often suggest password managers as one of the best measures for the end-users. However, the end-users have shown reluctance in adopting them, mostly due to the trust factor. The purpose of the paper was to examine the relationship of initial trust, and it's antecedents with the password manager's adoption intention. In this regard, using the Initial Trust Model as a framework, data from 289 respondents (age 18-35) were collected through a crowdsourcing website and analyzed using structural equation modeling (SEM) in SmartPLS 3.2. Results show that initial trust has a significant effect on the intention to adopt a password manager. In initial trust formation, firm reputation and structural assurances play a significant role, whereas personal propensity to trust does not significantly relate to initial trust. Moreover, firm reputation and structural assurances indirectly affect intention to adopt password managers.

© 2021 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the Conference Program Chairs.

Keywords: firm reputation; information security; initial trust; password managers; technology acceptance model; TAM; initial trust model

1. Background

The username and password combination have long been used as a form of authentication, and despite all the well-known problems related to passwords, it remains a dominant choice [1]. Security professionals recommend users to create passwords that are hard to guess (strong) and are not reused across different accounts (unique) [2]. Other recommendations include changing passwords at regular intervals and not writing them down or storing them

* Corresponding author. Tel.: +3-582-333-8647
E-mail address: alifar@utu.fi

1877-0509 © 2021 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2021.03.036

on users' phones or computers [3]. The four pieces of advice, when recommended together, can put users in a tricky situation. The passwords that are hard to guess for attackers can also be complicated for users to remember. As the number of accounts grows, which is the case today, the users are required to create and remember many more passwords than before. The situation further worsens when users are asked to change their passwords at regular intervals and not to note them anywhere. Together all this creates a lot of cognitive burden on the users [4]. This may lead to users creating weaker passwords that are easy to remember [5] and reusing them across different accounts [6]–[8], creating problematic issues in terms of both security and usability.

Security professionals recommend password managers (also referred to as password management applications) as a solution to the above-stated issues (create unique and strong passwords and change them frequently) [2], [9]. A password manager is a tool, a software application that alleviates the users' cognitive burden of creating and remembering many unique credentials, such as usernames and passwords, by creating, storing, and auto-filling required credentials where required [10]. It creates unique, strong passwords (which makes no sense to the naked eye), in light of desired rules, such as length, type of characters, and any other special attributes, for every account. Given the promising nature, password managers are actually one of the most often applied measures among security professionals for their online safety [9]. However, password managers have not achieved the same popularity among regular end-users. For example, back in 2015, when password managers were one of the top 5 measures applied by security professionals, only 24% of regular users were found to be using a password manager [2]. The situation seems even worse today as recent studies comparing security practices of security professionals and users show that only 3% of respondents use a password manager [9], [11].

To understand the reasons for the unpopularity of password managers among regular end-users, researchers conducted studies to identify the factors that inhibit users from using a password manager. Among the handful of available studies focused on regular end-users [12]–[15], trust has been found as one of the main reasons for the (non)adoption of password manager applications. Maclean and Ophoff [16], while determining key factors affecting the adoption of password managers, found that trust has a positive impact on the intention to adopt password managers. Few other studies, such as [14], [15], found that individuals do not adopt a password manager due to a lack of trust. Therefore, trust has been suggested as the first step towards increasing password managers' adoption [17]. While trust has been found to be a major factor towards password manager adoption, it is not yet investigated how trust can be established. To this end, it is crucial to understand the factors that improve trust and further their relations with adoption.

Trust is a complex phenomenon, and to establish trust between an individual and an artifact, it is crucial to understand how trust is formed and how it can be improved. McKnight et al. [18] showed that trust forms in phases. The trust-building process starts when individuals come across an unfamiliar artifact, having no or little information. Whatever information they have is not from personal experience. This initial phase is termed as initial trust [19], [20], which is affected by institutional, personal, and environmental factors [19], [21]. Once initial trust is established, individuals go through personal experience, try the artifact, and then decide to accept or reject it [19]. Thus, trust that is established after the use of an artifact is different from the initial trust that establishes before the use of an artifact. Therefore, initial trust plays a crucial in building up trust between a user and an artifact – which can be a service, an application, or a piece of software. So, we contend that initial trust formation is more relevant to understand in password managers' context.

In this paper, we examine the factors affecting initial trust and their relationship with users' intention to adopt password managers. In this regard, we use an online survey to collect data from 289 European young adults (aged 19-35) through a crowdsourcing platform and used structural equation modeling (SEM) in SmartPLS.

2. Theoretical background

McKnight et al. [18], [20] proposed a model called the initial trust model (ITM), outlining the three forces affecting initial trust: personal, institutional, and environmental. The user's personality, such as personal propensity to trust, significantly affects initial trust [21], [22]. Different institutional characteristics such as size, capability, integrity, role in the market, benevolence, reputation and/or brand may also affect a user's perception of an institution's services or products [19]. Environmental forces, such as structural assurance, enhance service

trustworthiness. Structural assurances include the availability of service guarantees, privacy policies, third party recognition, and endorsement [23]–[25].

2.1. Hypotheses development

The personal propensity to trust reflects an individual's tendency to trust others in various situations [18], [19]. This tendency is part of a person's personality and develops during the early stage of a person's life [26]. Trust propensity takes two forms [18]: faith in humanity and trusting stance. In the first form, a person believes people are reliable, and the second form depicts a person's belief that they will be better off when they consider people reliable. In line with previous studies [27], we suggest that personal propensity to trust in password managers will depict the degree to which individuals have a trusting stance towards the password managers. The following hypothesis is proposed:

H1: Personal propensity to trust will affect initial trust in password manager

Structural assurances, in general, are the safeguards, for example, promises, contracts, regulations or guarantees, provided by the institutions to their customers [22]. In a technological context, these safeguards are encryption, secure processes and procedures [28], third party certifications [29], and feedback mechanism [30]. In the case of password mangers, users are concerned about their data and seek guarantees such as mentioned above. Based on this we propose, the following hypothesis:

H2: Structural assurances will affect initial trust in password manager

Quality of service cannot be determined without prior experience. In this situation, when an individual does not have prior experience, referrals and word of mouth are the channels that influence an individual's perceptions. The individual's perceptions are also affected by institutional cues [25]. A good reputation is an assurance of a firm's integrity and goodwill, which increases potential customers' trust even when they have no previous experience with the service provider [31], and reduces the uncertainty and risks associated with the application [22]. We propose that the firm reputation of password managers will have a significant influence on the initial trust related to password managers and the following hypothesis is proposed:

H3: Firm reputation will positively affect initial trust in password managers

As discussed earlier, initial trust reduces the uncertainty and risk and establishes a connection that leads to the usage of a new application. Both perceived usefulness and initial trust affect behavioral intention [32]. Studies have shown that both these factors significantly affect adoption intention [33], thus, we propose the following hypotheses for this study:

H4: Initial trust positively affects intention to adopt password managers

Figure 1 shows the research model of the study. In addition to the above hypotheses, we will also examine the indirect effects of antecedents of initial trust on password managers' adoption intention.

3. Methodology

3.1. Procedure

Data for the study was collected using an online survey using an online platform Webropol. Participants for the study were recruited through an online crowdsourcing forum called SurveyCircle. Crowdsourcing platforms have been extensively used in usable security and HCI research and proven as an effective way of collecting data from random respondents [34]. SurveyCircle has been used previously in similar studies [35].

A three-part online survey was used for the data collection. Section 1 introduced participants with the purpose of the study, the requirement (European resident, at least 18 years of age), and time to complete the survey, and lastly, explicit consent was taken.

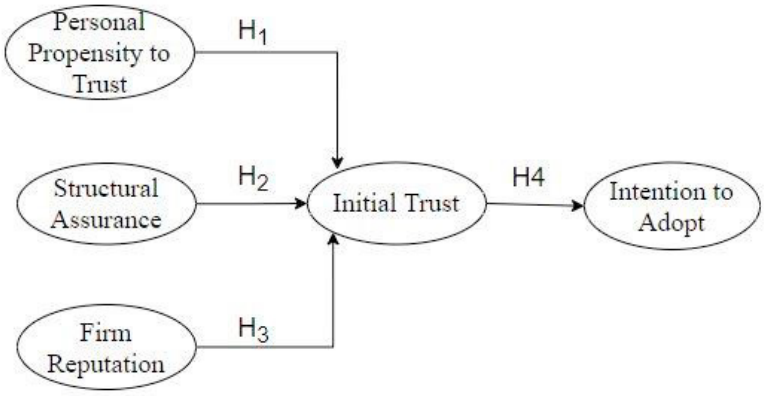

Figure 1. Research model explaining the relationship of antecedents of initial trust and initial trust's relation with intention to adopt password managers

After the consent, the respondents were asked to watch a short video (URL: https://www.youtube.com/watch?v=LrazAxl9Prs&t=3s) explaining the concept and features of the password manager. This video was shown to ensure that respondents have a uniform conception of password managers when responding to the statements in the survey. After the video, the respondents were asked if they had used a password manager. This question allowed us to identify and remove respondents who were or had been a password manager user. This step was necessary, as our purpose was to assess the initial trust and not the trust that formulates after the experience. In section 2, items measuring the constructs shown in figure 1 were presented. All the items were measured on a five-point Likert scale (1: strongly disagree to 5: strongly agree). The items, along with their sources, are given in Table 1. Finally, in section 3, questions related to demographics (age, gender, educational background, and country of residence) and background questions (number of accounts the participants manage passwords for, perceived computer skills, computer and internet experience) were asked.

3.2. Participants

A total of 1454 respondents visited the survey link. Out of which, 312 completed the survey. Out of 312, 23 responses were removed due to incomplete responses. 63% of the respondents were female, 35% were male, and the rest preferred not to tell. The average age of participants was 24.63 (SD = 2.09). 45% of participants have a high school or equivalent qualification, while the rest had a bachelor or equivalent degree. In terms of disciplines, 16% of participants were business students, 17% had an engineering background (including computer engineering), 15% were from medicine and natural sciences, 26% were from social sciences, education and 16% from the humanities and education. 48% of respondents were from the Nordic countries, 34% were from Western Europe, and the rest were from other parts of Europe. In terms of computer skills, 18% rated themselves at a basic level, 56% rated them as intermediate level users, while 26% considered themselves advanced level users. 35% of respondents had 1-5 accounts, 46% had 5-10 accounts, and 16% had ten or more accounts. The participants' computer and Internet experience was measured in years. 28% of the participants had 1-10 years of computer experience, 38% had 10-15 years, 28% had 15-20 years, while the rest had 20 or more years of experience. 36% of the participants had been using the Internet for 1-10 years, 43% for 10-15 years, 19% for 15-20 years, and the rest for 20+ years.

4. Data analysis and results

For initial screening, Statistical Package for Social Sciences (SPSS) v25.0 was used, whereas, later, for hypotheses testing, we used partial least square structural equation modeling (PLS-SEM) in SmartPLS v3.2 [36]. PLS-SEM is particularly useful when the sample size is small, data have normality issues, and the nature of the study is exploratory

[36], [37]. PLS-SEM analysis takes place in two steps: first, the measurement model is tested to ensure the quality of the variables in terms of reliability and consistency; second, the structural model is tested to understand relationships between the variables with the help of path coefficients (β) and coefficient of determination (R^2) and significance (p). We also examined the indirect effects to examine the effect of antecedents on the intention to use password managers. For significance testing, we used 5000 subsamples with a complete bootstrapping procedure.

4.1. Measurement model testing

Internal consistency was conventionally measured using Cronbach's alpha (α). However, composite reliability (CR) is prescribed as a better measure of internal consistency in PLS [37]. The recommended threshold for both α and CR is 0.7 [36]. In our study, α and CR for all the variables were between 0.73 and 0.913, and as suggested by [36], we have reported both α and CR. The items' reliability is assessed with the help of item loading on the respective variable, which should be > 0.60 [36]. In our study, most of the items had item loadings above the threshold except for one item from structural assurances (SA3). Convergent validity is assessed through the average variance explained (AVE) with a recommended threshold of 0.5 [36] . All our variables had AVE between 0.592 and 0.756. Lastly, for the assessment of discriminant validity, we used the Fornell-Larcker criterion [38]. Our variables met the said criterion, that the square root of AVE was higher than the correlation coefficients of the given two variables. Also, we also assessed collinearity using the variance inflation factor (VIF) with a threshold of five [36]. Only one item (IA3) from intention to adopt had collinearity issues (VIF>5) and was removed from further analysis. Table 1 has the measurement model testing results.

Table 1. Measurement model testing results, along with items and their sources

Constructs, items and sources	VIF	IL	α	CR	AVE
Personal Propensity to Trust [33], [39]			0.76	0.86	0.67
PPT1- I avoid the use of new products like password management software	1.42	0.72			
PPT2-I avoid the use of technology to manage passwords	1.94	0.91			
PPT3-I am cautious in using new technology to manage my passwords	1.60	0.81			
Structural Assurance [33], [39]			0.73	0.84	0.65
SA1- Password management software firms guarantee the protection of users' personal information	1.51	0.81			
SA2- I do not have a risk of personal information theft using password management software	1.33	0.72			
SA3- Password management software firms publish a policy on the protection of users' data	*1.09*	*0.45*			
SA4- My data is secure when I use password management software	1.69	0.87			
Firm Reputation [33], [39]			0.82	0.88	0.59
FR1-Password management software firms have a good reputation	2.59	0.73			
FR2-I trust the company that develops password management software	2.94	0.80			
FR3-The services password manager provides are of great quality	3.01	0.78			
FR4-The company that produced the password manager I use is a secure institution	2.86	0.76			
FR5-Password management software firms offer good services	2.33	0.75			
Initial Trust [33], [39]			0.87	0.90	0.66
IT1-Password management software always provides accurate service	1.74	0.66			
IT2-Password management software provides safe services	2.64	0.82			
IT3-Password management software provides reliable services	3.33	0.87			
IT4-Password management software seems reliable	3.87	0.84			
IT5-Password management software seems secure	3.96	0.84			
Intention to Adopt [33], [39]			0.87	0.91	0.72
IA1-I have the intention of managing my passwords by using the password management software	3.80	0.89			
IA2-I'm curious about password management software	1.48	0.68			
IA3-I have the intention of managing my accounts using a password management software	*5.90*	*0.94*			
IA4-I have the intention of logging in with the help of a password management software	3.47	0.90			
IA5-I plan to use a password management software	3.99	0.91			

Note: Items shown in italic were removed from further analysis

4.2. Structural model testing

Once the reliability and validity of the variables were established, we ran the structural model to test the proposed hypotheses (1 to 4). Table 2 shows the result of the structural model test. Out of four hypotheses, three were supported. In our model, 59% of variance in initial trust is explained by structural assurance ($\beta = 0.38$, $p < 0.001$)

and firm reputation (β = 0.44, p < 0.001); and 11% of variance in intention to adopt is explained by initial trust (β = 0.33, p < 0.001).

As a post hoc analysis, we also examined the total indirect effects of independent variables on the dependent variable (intention to adopt password managers). Structural assurance (β = 0.12, p < 0.001) and firm reputation (β = 0.14, p < 0.001) had a significant indirect impact on intention to adopt password manager; whereas, personal propensity to trust, did not have a significant indirect effect (β = -0.01, p = 0.71) on the intention to use password managers.

Table 2. Structural model testing results showing significant and non-significant relations.

Hypothesis	Relationship	*β*	*t*	*p*	f^2	*Result*
H1	*PPT→IT*	*-0.03*	*0.450*	*0.688*	*0.002*	*Not supported*
H2	SA→IT	0.38	4.760	<0.001	0.21	Supported
H3	FR→IT	0.44	4.484	<0.001	0.20	Supported
H4	IT→IA	0.33	6.250	<0.001	0.13	Supported

Note: PPT=personal propensity to trust, SA=structural assurance, FR=firm reputation, IT=initial trust, IA=intention to adopt, *β*=path coefficient, *t*= t-statistics. p= significance, f^2 =*effect size.* Insignificant relationships are shown in italic.

5. Discussion

This study examined the factors that constituted initial trust in password managers and further investigated the effect of initial trust on the adoption intention of password managers. The study provides interesting insights of the factors that result in the formation of initial trust in password managers.

To identify the factors that play a significant role in forming an initial trust, we examined the effect of three selected factors: firm reputation, structural assurances, and personal propensity to trust. The results (Table 1) indicate that there is structural assurance and firm reputation significantly affect initial trust formation (together, they explain 59% of initial trust variance). On the other hand, the personal propensity of trust does not significantly affect initial trust. While the previous studies [12], [40] identified a lack of trust as one of the major problems towards adopting a password manager, these do not talk about the initial trust. Given that our study is among the first, if not the first, to study the formation of initial trust in password managers' adoption intention, we cannot compare our results with previous studies on password managers. A fruitful discussion is possible in the future when further studies will examine initial trust formation in password managers.

Among the three identified antecedents, structural assurances outweigh both firm reputation and personal inclination towards initial trust. The structural assurance measures the vendors' related measures of giving a guarantee of protecting the users' personal information, having an open privacy policy, and having measures for data security. This highlights the perceived importance of safeguard measures taken by password managers vendors. The findings above indicate that individuals will be more willing to trust password managers when the vendor is reputed and provides assurances against the possible risks. Considering that personal propensity to trust does not play a significant role in developing initial trust in the password manager, individuals do not seem to oppose password managers in general due to their personality traits.

The antecedents of initial trust also affect intention to adopt password managers. We found that both firm reputation (β = 0.11, p < 0.001) and structural assurances (β = 0.10, p < 0.001) significantly affect password manager's adoption intention indirectly. The results also suggest that respondents give equal importance to both structural assurance and firm reputation.

5.1. Implications

This study makes important contributions to research and practice. For researchers, the model provides an understanding of how initial trust in password managers is formed and further their relation with the adoption intention of password managers. Previous studies show that people avoid using password managers due to the trust factor and trust relationship with password manager adoption [16], [41]. This study showed how initial trust is formed. Initial trust can further lead to trust-building in password managers and positively impact their adoption. This study utilizes ITM to understand password manager adoption, which is an addition to the current knowledge

base that utilizes UTAUT[16] and the Protection Motivation Theory (PMT) [41] models to understand password manager adoption.

The study highlights the importance of firm reputation as well as structural assurances. Therefore, the vendors should focus on establishing a trusting relationship with the customers from the early stage. One way to do this is to run marketing campaigns highlighting the vendors' privacy policies and safeguards to prevent any loss of information and confidentiality.

5.2. Limitations and future work

This study is not without limitations. First, the study participants were mostly located in Northern and Western Europe and may not represent the whole EU in terms of the young adult population. The survey was conducted in English, so there might be some ambiguity among the respondents considering English is not an official language in most EU countries. In the study, we framed generic questions aiming at standalone password manager applications. Since results show that both structural assurance and firm reputation equally affect intention to adopt password managers, a future study may consider seeing differences between users of different password managers. We did not measure structural assurances such as compensation for losses or external protection, such as a vendor's assurance to comply with regulations and laws. We cannot know from the current study how powerful compensation for the losses and compliance to regulations would affect an individual's initial trust in password managers. A future study may clarify their roles.

Since social norms affect trust [22], it will be interesting to see the role of social norms as antecedent of initial trust and password manager adoption. Moreover, studies may also consider other factors that may play an important role in initial trust formation. One such factor is the awareness of password managers. Awareness has been found as a driving force for learning skills necessary for enacting a certain type of behavior [42]. We should also look into gender differences as previous studies found a gender disparity in the formation of trust [43], [44], as well as in security behavior [45]. We also believe that integration of two or more models (For example, [27], [33], [37] and [46]) may further enhance our understanding of password managers' adoption.

6. Conclusion

In this study, we examined the formation of initial trust in password managers' context and how initial trust relates to password manager adoption intention. We proposed a research model based on the initial trust model and technology acceptance model. To test the model empirically, data were collected from 289 young adults from Europe (aged 18-35). The analysis was mainly carried out using structural equation modeling (SEM) in SmartPLS3.2 and supported by SPSS v25.0. The results show that structural assurance ($\beta = 0.38$, $p < 0.001$) and firm reputation ($\beta = 0.44$, $p < 0.001$) play a significant role in initial trust formation. Further, initial trust affects the intention to adopt a password manager. This study is among the first studies to explain the factors affecting password managers' initial trust and how it translates to password managers' adoption intention.

7. References

[1] Bonneau, Joseph, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. (2012) "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes." In *2012 IEEE Symposium on Security and Privacy* 553–67.

[2] Ion, Iulia, Rob Reeder, and Sunny Consolvo. (2015) "'...No One Can Hack My Mind': Comparing Expert and Non-Expert Security Practices." In *2015 Symposium on Usable Privacy and Security* 327–40

[3] Reeder, Robert, Iulia Ion, and Sunny Consolvo. (2017) "152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users." *IEEE Security & Privacy* **15 (5)**: 55–64.

[4] Renaud, Karen. (2012) "Blaming Noncompliance Is Too Convenient: What Really Causes Information Breaches?" *IEEE Security & Privacy* **10(3)**:57–63.

[5] Dell' Amico, Matteo, Pietro Michiardi, and Yves Roudier. (2010) "Password Strength: An Empirical Analysis." *In 2010 Proceedings IEEE INFOCOM* 1–9.

[6] Das A, Bonneau J, Caesar M, Borisov N, Wang X. (2014)The Tangled Web of Password Reuse. In: *NDSS* p. 23–6.

[7] Florencio, Dinei, and Cormac Herley. (2007) "A Large-Scale Study of Web Password Habits." *In Proceedings of the 16th International*

Conference on World Wide Web - WWW '07 p. 657.

[8] Pearman, Sarah, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. (2017) "Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat." *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17* p. 295–310.

[9] Busse, Karoline, Julia Schäfer, and Matthew Smith. (2019) "Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice." *In Fifteenth Symposium on Usable Privacy and Security (SOUPS)* p. 117–36.

[10] Oesch S, Ruoti S. (2020) That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Thirteen Password Managers. In: *USENIX Security Symposium* p. 2165-2182

[11] Farooq A. In Quest of information security in higher education institutions : Security awareness, concerns and behaviour of students. Doctoral Dissertation. University of Turku, Turku; 2019 [cited 2019 Dec 29]. Available from: https://research.utu.fi/converis/mypages/browse/Publication/42654823

[12] Karole, Ambarish, Nitesh Saxena, and Nicolas Christin. (2011) "A Comparative Usability Evaluation of Traditional Password Managers." In *13th International Conference on Information Security and Cryptology*, edited by D. Rhee, KH., Nyang, 233–51.

[13] Lyastani, Sanam Ghorbani, Michael Schilling, Sascha Fahl, Michael Backes, and Sven Bugiel. (2018) "Better Managed than Memorized? Studying the Impact of Managers on Password Strength and Reuse." In *27th USENIX Security Symposium* p. 203–20.

[14] Fagan, Michael, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. (2017) "An Investigation into Users' Considerations towards Using Password Managers." *Human-Centric Computing and Information Sciences* **7(1)**:12.

[15] Aurigemma, Salvatore, Thomas Mattson, and Lori Leonard. (2017) So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications? In: *50th Hawaii International Conference on System Sciences* p. 4061-4070.

[16] Maclean, Raymond, and Jacques Ophoff. (2018) Determining Key Factors that Lead to the Adoption of Password Managers. In: *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)* p. 1–7.

[17] Ganai, Omar, and Steven Ledbetter. (2018) How to Increase Adoption and Use of Password Managers. 2018 [cited 2019 Aug 19]. Available from: https://medium.com/practical-motivation-science/how-to-increase-adoption-and-use-of-password-managers-41d242971c96

[18] McKnight, D. Harrison, Larry L. Cummings, and Norman L. Chervany. (998) Initial trust formation in new organizational relationships. *Academy of Management Review* **23(3)**:473-90.

[19] McKnight, D. Harrison, Vivek Choudhury, and Charles Kacmar. (2002) Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research* **13(3)**:334-59.

20. McKnight DH, Chervany NL. (2001) Trust and distrust definitions: One bite at a time. In *Trust in Cyber-societies* 27-54. Springer, Berlin, Heidelberg.

[21] Gefen, David. (2000) E-commerce: the role of familiarity and trust. *Omega* **28(6)**:725-37.

[22] Li, Xin, Traci J. Hess, and Joseph S. Valacich. (2008) Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems* **17(1)**:39-71.

[23] Rousseau, Denise M., Sim B. Sitkin, Ronald S. Burt, and Colin Camerer. (1998) Not so different after all: A cross-discipline view of trust. *Academy of Management Review* **23(3)**:393-404.

[24] Lu, Hsi-Peng, and Philip Yu-Jen Su. (2009) Factors affecting purchase intention on mobile shopping web sites. *Internet Research* **19(4)**: 442-458.

[25] Kim, Kyung Kyu, and Bipin Prabhakar. (2004) Initial trust and the adoption of B2C e-commerce: The case of internet banking. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* **35(2)**:50-64.

[26] Lee, Matthew K. O., and Efraim Turban. (2001) A trust model for consumer internet shopping. *International Journal of Electronic Commerce*. **6(1)**:75-91.

[27] Afshan, Sahar, and Arshian Sharif. (2016) Acceptance of mobile banking framework in Pakistan. *Telemat Informatics* **33(2)**:370–87.

[28] McKnight, D. Harrison, and Norman L. Chervany. (2000) What is trust? A conceptual analysis and an interdisciplinary model. *AMCIS 2000 proceedings* 827-32

[29] Luo, Xueming. (2002) Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management* **31(2)**:111-8.

[30] Pavlou, Paul A., and David Gefen. (2004) Building effective online marketplaces with institution-based trust. *Information Systems Research* **15(1)**:37-59.

[31] Lohse, Gerald L., and Peter Spiller. (1998) Electronic shopping. *Communications of the ACM* **41(7)**:81-7.

[32] Fishbein, Martin., and Icek Ajzen. (1975) Belief, attitude, intention, and behavior : an introduction to theory and research. Addison-Wesley Pub. Co . 578 p.

[33] Kim, Gimun, BongSik Shin, and Ho Geun Lee. (2009) Understanding dynamics between initial trust and usage intentions of mobile banking. *Information Systems Journal* **19(3)**:283-311.

[34] Redmiles, Elissa M., Sean Kross, and Michelle L. Mazurek. (2019) How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. *Proceedings of IEEE Symposium on Security and Privacy* p. 1326–43.

[35] Fietkiewicz, Kaja, and Aylin Ilhan. (2020) Fitness Tracking Technologies: Data Privacy Doesn't Matter? The (Un)Concerns of Users, Former Users, and Non-Users. *Proceedings of the 53rd Hawaii International Conference on System Sciences* p. 3439–48.

[36] Hair Jr, Joseph F., G. Tomas M. Hult, Christian Ringle, and Marko Sarstedt. (2006) A primer on partial least squares structural equation modeling (PLS-SEM). Sage Publishers.

[37] Henseler, Jörg, Christian M. Ringle, and Rudolf R. Sinkovics. (2009) The use of partial least squares path modeling in international marketing. *In New challenges to international marketing* 277-319

[38] Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*. 1981. **18(1)**:39-50.

[39] Oliveira, Tiago, Miguel Faria, Manoj Abraham Thomas, and Aleš Popovič. (2014) Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. *International Journal of Information Management* **34(5)**:689-703.

[40] Chiasson, Sonia, P C Van Oorschot, and Robert Biddle. (2006) A Usability Study and Critique of Two Password Managers. *15th USENIX Security Symposium* p. 1–16.

[41] Aurigemma, Salvatore, Thomas Mattson, and Lori N K Leonard. (2019)Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications. *AIS Transaction on Replication Research* **5(3)**:1–21.

[42] Farooq, Ali, Debora Jeske, and Jouni Isoaho. (2019) Predicting Students' Security Behavior Using Information-Motivation-Behavioral Skills Model. *In IFIP International Conference on ICT Systems Security and Privacy Protection* p. 238-252. Springer, Cham.

[43] D. Gefen and D. W. Straub. (1997) "Gender differences in the perception and use of e-mail: An extension to the technology acceptance model," *MIS Quarterly.* , **21(4):** 389–400

[44] R. Riedl, M. Hubert, and P. Kenning. (2010) "Are there neural gender differences in online trust? An fMRI study on the perceived trustworthiness of eBay offers," *MIS Quarterly.* 34 (SPEC. ISSUE 2), pp. 397–428

[45] Farooq, Ali, Johanna Isoaho, Seppo Virtanen, and Jouni Isoaho. (2015) Observations on genderwise differences among university students in information security awareness. *International Journal of Information Security and Privacy (IJISP)* **9(2)**:60-74.

[46] Farooq, Ali, Joshua Rumo A. Ndiege, and Jouni Isoaho. (2019) "Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior." *2019 IEEE AFRICON*.