Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs

Nora Alkaldi
University of Glasgow, Glasgow, U.K.
n.alkaldi.1@research.gla.ac.uk

Karen Renaud
Abertay University, Dundee, U.K.
k.renaud@abertay.ac.uk

Lewis Mackenzie
University of Glasgow, Glasgow, U.K.
lewis.mackenzie@glasgow.ac.uk

Abstract

Password managers are a potential solution to the password conundrum, but adoption is paltry. We investigated the impact of a recommender application that harnessed the tenets of self-determination theory to encourage adoption of password managers. This theory argues that meeting a person's autonomy, relatedness and competence needs will make them more likely to act. To test the power of meeting these needs, we conducted a factorial experiment, in the wild. We satisfied each of the three self-determination factors, and all individual combinations thereof, and observed short-term adoption of password managers. When all self-determination factors were satisfied, adoption was highest, while meeting only the autonomy or relatedness needs individually significantly improved the likelihood of adoption.

1. Introduction

The alphanumeric password is still the dominant user authentication approach. This human propensity to choose weak passwords has been the thorn in the security professional's side ever since computer users first started using passwords [1]. Researchers have tried to improve password practice [2, 3, 4], but the problem is proving intractable. People find the general password concept burdensome, primarily due to memory load [5], and they cope by choosing weak passwords or offset memory load by writing down or reusing them [6].

Password managers solve both security and usability problems by removing the need for people to memorize a large number of strong passwords. Many password manager applications exist, and have been available since 1999 [7]. They store passwords securely; protected by a strong master key. This allows users to amortize the effort they expend memorising a strong master key, because it does not *have* to be changed. Password managers effectively shoulder the password burden on the user's behalf, and make it easy for them to deploy strong passwords across all their accounts, because the primary driver behind password reuse is eliminated.

Despite the obvious benefits, these tools have not been widely adopted [8]. Low adoption also manifests for other usable security tools, such as fingerprint-enabled unlocking on Smartphones [9]. If we are able to find a mechanism for encouraging password manager adoption, it might be possible to use the same mechanism to encourage the adoption of other security tools too.

Researchers are turning to behavioral change theories to determine how to exert influence to persuade people to behave in a particular way [10]. In this paper, we report on an investigation into the impact of a password manager recommender system that satisfied the three core tenets of Self-Determination Theory: *autonomy, relatedness* and *competence* [11]. Our purpose was to determine whether meeting these needs, either all or in different combinations, would improve password manager uptake.

Prior work is reviewed in Section 2. Section 3 outlines the hypotheses and Section 4 presents the study design. The analysis is detailed in Section 5. Our main findings and limitations are presented in Section 6 and Section 7 concludes.

2. Related & Background Research

Password Managers: Alphanumeric passwords have great potential for strength but fail in the hands of a heterogeneous users from all walks of life, because people choose weak passwords. Some solutions attempt to encourage stronger password choice [12]. Others suggest alternatives such as graphical passwords [13] or biometrics [14]. However, such alternatives require major changes to existing systems and are also personally risky for developers because they are not the *de facto* authentication standard.

Password managers avoid password-related effort [15]. Commercially-available password managers can be classified into three types: (a) built into the web browser (*e.g.* Google Chrome), (b) stand-alone or ded-

URI: https://hdl.handle.net/10125/59920
ISBN: 978-0-9981331-2-6

icated (*e.g.* LastPass) and (c) browser extensions (*e.g.* LastPass and Dashlane). Most stand-alone password managers are also available as browser extensions (*e.g.* LastPass).

Password managers store their passwords in three different ways: (1) locally (*e.g.* Keepass), (2) cloud/web-based, (*e.g.* LastPass), and (3) no-storage or hashing (*e.g.* PwdHash).

Password managers re-establish a reasonable balance between the security and usability of passwords, enjoying research attention [16, 17, 18, 19]. Most of the existing research on password managers has focused on (1) technical aspects of these tools and mechanisms to improve their security and usability [16, 17], (2) evaluating their security [18, 19], or (3) designing for usability [20]. Less work has been carried out on password manager adoption.

One of the few first studies considering the users' perspective in using a password manager was published in 2006 by Chiasson *et al.* [21]. They conducted a usability study of two desktop password managers: PwdHash and Password Multiplier. They discovered incorrect or incomplete mental models related to password managers, and also identified usability issues affecting the participants' ability to use these tools securely. Karole *et al.* [22] conducted a usability study comparing three password managers: LastPass (an online password manager), KeePassMobile (mobile-phone password manager) and Roboform2Go (portable USB password manager). Their research showed that although the online password manager was the easiest to use, users preferred to use the other two portable password managers. There are clearly a number of password manager-specific factors at play here, making password manager adoption different from adoption of other kinds of software tools.

Human Motivation: Security is considered a secondary task by end users [23]. That being so, they try to avoid engaging with security, especially if it gets in the way of their primary goal [24]. Blaming users for not using security measures is not an effective way to enhance security [5]; system designers need to try to understand the root causes of these behaviors, and to design security systems with the user's needs, capabilities and proclivities in mind [25]. Researchers suggest that non-use is due to underestimation of the riskiness of insecure behaviors [26]. Another explanation is that people have a "compliance budget" [27] which can be exhausted. Herley [28] suggests that users make a rational decision to adopt security measures when the cost-benefit outcome of adopting these systems outweighs the cost-benefit outcome of not adopting them. Another perspective is to consider human motivation. Broadly speaking, human motivation is either: *extrinsic* or *intrinsic* [29]. The former refers to the desire for rewards, such as money. *Intrinsic* motivation drives someone to perform an activity for the pleasure and satisfaction derived from engaging in the activity itself. Existing research on human behavior found the second type to be far more effective in motivating individuals to act in a particular way [30]. Accordingly, individuals engage in a range of behaviors, for which there is no extrinsic motivation, such as sharing knowledge [31] or donating blood [32]. A myopic focus on extrinsic motivational interventions, when it comes to encouraging security behaviors, might well be neglecting far more effective interventions [33]. Researchers in non-security disciplines are already realising this [34].

Human motivations have been studied to explore individuals' behavior and mechanisms for encouraging the adoption of recommended behaviors [35] to help us to formulate interventions to improve adoption. Motivation theories such as *Self-Determination Theory* (SDT) [11], and Pink's Motivation Theory [36] can offer a theoretical framework for understanding such motivations.

According to SDT theory [11], three basic human psychological needs affect motivation with respect to an individual engaging in particular activity. *(1) Autonomy* is the desire to have control over one's own life and the need to be free to make choices based on personal decisions. *(2) Competence* refers to the feeling of having a sense of self-efficacy in carrying out a particular task. *(3) Relatedness* refers to feeling connected to others, to feel part of something or belonging to a larger community. This SDT theory has been applied in different sectors: *e.g.* education [37] and health care [38]. This theory has also been used to predict users' intention to protect information security [39].

The research reported here sought to investigate the impact of interventions that aimed to satisfy self-determination needs in order to influence Smartphone password manager adoption.

Security Behavior Investigations: Some researchers investigate security behavior based on self-reported data collected with questionnaires [40, 9]. This method is particularly appropriate in initial studies into a phenomenon because they are able to elicit responses from a large population. A questionnaire can be distributed widely and cheaply. However, the reliability of self report is debatable, because people are not always entirely frank in their responses [41].

Another method used for studying information security-related behaviors is lab-based experiments [42, 21]. Most such laboratory experiments are solely focused on exploring particular aspects of a security tool such as usability for example. [42, 21]. Such studies are essential in making sure that users do not encounter undue difficulties using the tool, but because we know that usability is not the only precursor of adoption, we need to do more than usability testing.

Another method is to observe actual security behaviors [43, 44]. For example, Machuletz *et al.* [43] applied the Theory of Reasoned Action to investigate the determinants that lead notebook users to cover their webcams and cameras. This method is more reliable than the others, in terms of uncovering genuine security-related behaviors. It is indeed challenging to use this method for all security-related behaviors, because security actions are solo and sensitive activities. Yet observation *does* deliver very valuable insights that are not possible to obtain as reliably via self report. Since the focus of this research required us to determine whether the participants *actually* installed a password manager, we used the observational method.

3. Hypotheses

The goal of this study is to test the effect of satisfying self-determination theory needs within a password manager recommender application, in terms of observable short-term adoption of a password manager.

Alkaldi and Renaud [8] report that actual password manager adoption comprises three stages: (1) *search*, (2) *decide*, and (3) *try*, the latter being indicative of short-term adoption. A recommender application will support users in searching and deciding, and then allow us to see whether a trial ensues. Long-term adoption is something that occurs over months and years and cannot occur without short-term adoption i.e. initial installation of the password manager. Hence this study is concerned with determining short-term adoption (i.e. the try stage). A future study will examine the factors impacting the long-term adoption.

We formulated the following hypotheses related to Smartphone password manager adoption.

The first two hypotheses are related to whether the recommender system makes a difference.

*H_a0: There is **no difference** in password manager adoption between participants who use a recommender system, and those who are merely informed of their existence.*

*H_a1: The mean number of password manager adoptions **is greater in the group who use a recommender system**, than in the group who are merely informed of their existence.*

The second set of hypotheses is related to the impact of self-determination need satisfaction:

*H_b0: A recommender application that meets a participant's **autonomy, competence and relatedness needs** does not change the incidence of password manager adoption.*

*H_b1: A recommender application that meets **autonomy** needs significantly increases password manager adoption.*

*H_b2: A recommender application that meets **competence** needs significantly increases password manager adoption.*

*H_b3: A recommender application that meets **relatedness** needs significantly increases password manager adoption.*

*H_b4: A recommender application that meets **competence** need significantly increases password manager adoption only if the **autonomy** need is also supported.*

*H_b5: A recommender application that meets **relatedness** need significantly increases password manager adoption only if the **autonomy** need is also supported.*

*H_b6: A recommender application that meets **relatedness** need significantly increases password manager adoption only if **competence** need is also supported.*

*H_b7: A recommender application that meets **relatedness** need significantly increases password manager adoption only if the **competence** and **autonomy** needs are also supported.*

4. Study Design

Over 250 password manager applications are listed in the Google Play Store. It is challenging for anyone to evaluate these applications to select the best possible one. We thus offered people a recommender app that matched their stated preferences to a subset of the available password managers. The app essentially eases the search process.

In order to test the hypotheses, a recommender system was developed, called ***CyberPal***, which made it possible for us to test self determination theory-based interventions.

Raising Awareness: The recommender's first role was to raise awareness of password managers. A previous study found that people are generally unaware of password managers [8], so an awareness video was included in the intervention. We used the same awareness video clip that was used by Aurigemma *et al.*'s study [45]. This video provides an overview of password managers, and the reason for using them, and details the attractive features of such tools, such as its usefulness and effectiveness. This video also includes messages calculated to increase the feeling of certainty with respect to using a password manager. Having ensured awareness, we proceeded to support *searching* and *deciding* stages.

The CyberPal Recommender Application: CyberPal was implemented as an Android Smartphone application. The user selects a number of preferred password manager features. (A number of features of password managers were identified in a separate study.) The recommender system then suggested one or more matching password managers for consideration based on the selected features.

Behavioral Intention: It is reasonable to assume that intention precedes trial, so it is necessary to measure participants' intention. A participant might have a pre-existing intention to use a password manager, and he/she then uses the recommender to find the one that suits him/her best. On the other hand, using CyberPal might help a person to formulate an intention to use a password manager. Furthermore, because the experiment was conducted in the wild, we expected that some participants would have perfectly valid reasons for forming a low, or no, intention to use a password manager. We thus measure behavioral intention on a 1-7 Likert scale [46]. We also asked for gender and age. After a week, a post-questionnaire popped up, asking participants to select reasons for choosing to use a password manager, or not, as the case may be.

Supporting Self Determination Needs: Features were added to the recommender to support the specific self determination theory needs dictated by each experimental group. First, the features that can be used to support each of the three needs were identified from the literature [47, 48, 49, 50, 51].

Autonomy: The use of non-controlling language [52, 53], acknowledging negative feelings [54, 53], and offering more than one options for the person to choose from [53], but not too many [55] all support autonomy.

CyberPal supports autonomy by: (1) offering choice, and (2) using non-controlling language. Phrases such as "*would you like..*" and "*you may...*" were used. Furthermore, providing more than one choice engenders a feeling of autonomy, but too many choices have a potentially negative effect. Three are recommended [56] (Figure 2).

Relatedness: The relatedness need can be supported by providing some kind of connectivity related to the target behavior [57]. It may constitute engendering a sense of community [58]. During the pre-adoption stage, being aware of other password manager adopters can support the relatedness basic need in this context [59]. Because password managers are critical systems, and relatively poorly known, being aware of the fact that your contacts are password manager adopters gives the CyberPal user a feeling that they are not alone (Figure 5).

Competence: Suggested strategies for meeting this need include: (1) offering clarity [60], (2) using positive feedback [61, 62], (3) providing guidance [60], (4) encouraging, and (5) supporting their beliefs that they can perform the target behavior without assistance [63]. A person might like the idea of a password manager, and want to use one, but be felled by uncertainty, which could deter them from trialing a password manager.

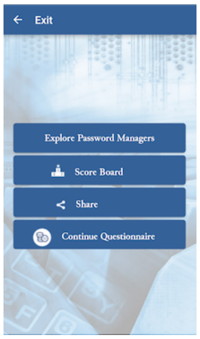
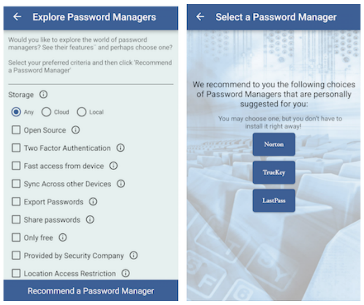


Figure 1. Main application Menu


← Explore Password Managers
← Select a Password Manager
Norton
TrueKey
LastPass
Recommend a Password Manager

Would you like to explore the world of password managers? See their features¨ and perhaps choose one?

Select your preferred criteria and then click 'Recommend a Password Manager'

Storage ⓘ

● Any ○ Cloud ○ Local

□ Open Source ⓘ

□ Two Factor Authentication ⓘ

□ Fast access from device ⓘ

□ Sync Across other Devices ⓘ

□ Export Passwords ⓘ

□ Share passwords ⓘ

□ Only free ⓘ

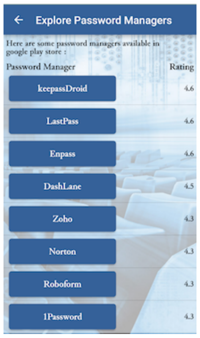
□ Provided by Security Company ⓘ

□ Location Access Restriction ⓘ

We recommend to you the following choices of Password Managers that are personally suggested for you:

You may choose one, but you don't have to install it right away!

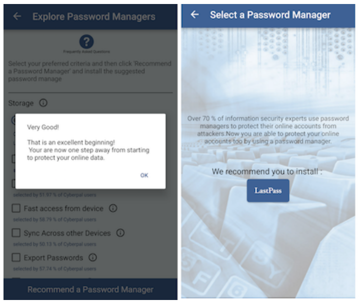
Figure 2. Meeting Autonomy Needs



Here are some password managers available in google play store :

Password Manager	Rating
keepassDroid	4.6
LastPass	4.6
Enpass	4.6
DashLane	4.5
Zoho	4.3
Norton	4.3
Roboform	4.3
1Password	4.3

Figure 3. Placebo Interface


← Explore Password Managers
Frequently Asked Questions
OK
Recommend a Password Manager
← Select a Password Manager
LastPass

Select your preferred criteria and then click 'Recommend a Password Manager' and install the suggested password manage

Storage ⓘ

Very Good!

That is an excellent beginning!
Your are now one step away from starting to protect your online data.

selected by 51.97 % of Cyberpal users

□ Fast access from device ⓘ
selected by 58.79 % of Cyberpal users

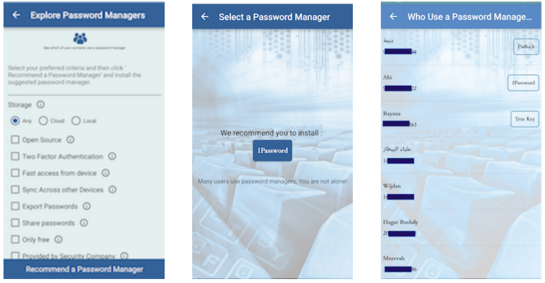
□ Sync Across other Devices ⓘ
selected by 50.13 % of Cyberpal users

□ Export Passwords ⓘ
selected by 57.74 % of Cyberpal users

Over 70 % of information security experts use password managers to protect their online accounts from attackers.Now you are able to protect your online accounts too by using a password manager.

We recommend you to install :

Figure 4. Meeting Competence Needs


← Explore Password Managers
See which of your contacts use a password manager
Recommend a Password Manager
← Select a Password Manager
1Password
← Who Use a Password Manage...
Padlock
1Password
True Key

Select your preferred criteria and then click ' Recommend a Password Manager' and install the suggested password manager.

Storage ⓘ

● Any ○ Cloud ○ Local

□ Open Source ⓘ

□ Two Factor Authentication ⓘ

□ Fast access from device ⓘ

□ Sync Across other Devices ⓘ

□ Export Passwords ⓘ

□ Share passwords ⓘ

□ Only free ⓘ

□ Provided by Security Company ⓘ

We recommend you to install :

Many users use password managers. You are not alone!

ديمة
[redacted]

Abi
[redacted]

Rayana
[redacted]

علياء البيطار
[redacted]

Wijdan
[redacted]

Hagar Rushdy
[redacted]

Mneerah
[redacted]

Figure 5. Meeting Relatedness Needs

CyberPal provides a "frequently-asked questions" button to reduce uncertainty. A positive feedback message is displayed when the user submits their preferences, to encourage them to proceed to short term adoption. Information about the most desired features chosen by other CyberPal users is also provided (Figure 4).

Platform: The target population was Android Smartphone users. Android was chosen as a platform because it is used by over 80% of Smartphone users worldwide, as compared to other Smartphone operating systems [64, 65].

Testing: The CyberPal application was tested extensively on 12 Android devices and then tested by a sample of 6 Android users to improve usability. Finally, the application was uploaded to the `Betafamily.com` testing service, where it was tested by 9 testers over a two week period. All feedback was used to improve the application.

Experiment Design: The experiment allowed us to test for the following:

(1) The effect of the password manager recommender system compared to only providing information about a password manager (Hypotheses $H_a(0,1)$), and

(2) The effect of supporting the three SDT needs, exhaustively testing all possible combinations (Hypotheses $H_b(0,1\text{-}7)$).

To avoid the experimental hazard of participants believing, or expecting, to install password manager, a placebo effect strategy was used i.e. an intervention that had no effect. In psychological experiments, researchers generally utilize a placebo control group: a group of participants who are exposed to a placebo or fake independent variable [66, 67, 68]. The impact of this non-intervention is then compared to the results of the real independent variable of interest. In the placebo case, CyberPal merely displayed information about password manager tools, as derived from the Android Play Store.

Furthermore, to test the impact of each of the three basic needs, a 2*2*2 factorial experiment design was used. Eight versions of the recommender system were deployed, each of which satisfied some combination of the three SDT needs (Table 1).

Participants were randomly assigned to one of the experimental or the placebo control groups (Table 1). This type of design can help to establish causation by determining cause and effect between variables. We can isolate the impact of each intervention on adoption behavior and determine which of the three independent variables, or their interactions, are more likely to influence adoption.

Placebo Group: (G1) this group used a version of CyberPal that was designed to raise awareness of password manager applications, without the recommender system. This establishes a baseline of how many people would adopt password managers merely because they became aware of them. They were simply shown a list of password managers from the Google Play Store.

Experimental Groups: (G2, G3, G4, G5, G6, G7, G8, G9): The participants used slightly different versions of the CyberPal recommender application. Each version supports the different combinations of *autonomy, competence* and *relatedness* needs.

Table 1. Experimental Group Need Satisfaction (Autonomy=A, Competence=C, Relatedness=R)

Recommender App	C		Not C	
	A	Not A	A	Not A
R	G8	G7	G6	G5
Not R	G4	G3	G2	G9
List of password managers (placebo): G1				

Ethical Considerations: The data we collected in the mobile application is privacy sensitive, and we took great care to respect participants' privacy. We conducted the study under University of Glasgow institutional review board approval. The participants' consent was obtained before collecting any data. We only report aggregate statistics, thereby ensuring participant anonymity.

Tasks: The participants of the CyberPal Android application were able to carry out the following tasks: (1) Install CyberPal; (2) Grant consent to participate in an experiment; (3) Register by their phone number and choose a user name; (4) Provide the contact number of the user who invited her/him, if applicable; (5) Complete a pre-questionnaire to provide demographic data and measure the intention to use a password manager; (6) Use CyberPal to explore password manager features; (7) Keep CyberPal on the device for a week; (8) Complete a post-questionnaire.

Recruitment: The CyberPal recommender application was launched in the Google Play Store at the end of June 2017. Any Android user could install the app and participate in the experiment, if they were happy to consent to allow the app to collect their data for the purposes of this research. Also, participants are likely to have told their friends about CyberPal. This recruitment technique can be used to recruit participants who are difficult to identify or have to meet certain criteria to support the study experiment. In our study, we needed participants who knew each other to support the relatedness satisfaction conditions in the experiment.

Invitations to participate were also sent to 219,221 Android users, using the Facebook advertising service, between July and September 2017. The invitation targeted English speakers, aged 18 or over, who owned an Android device with version 4 or above. To increase the likelihood of participation, the invitation was sent only when the device was connected to WiFi. Participants were enticed by offering them the chance to win one of five online vouchers of their own choice from one of: PayPal, Amazon or the Google Play Store.

To encourage participants to recruit other participants, specifically their friends (to support the relatedness need), participants were encouraged to invite others by giving them 10 points for each person who accepted their invitation to participate in the experiment. The total number of collected points for each participant is displayed on a scoreboard, accessible from the app's main menu.

Later, after the experiment concluded, all participants who completed their tasks entered the prize draw. The winner of £50 voucher was selected from the top 10%, then the winner of £30 was selected from the top 30%. Finally, three winners of £10 vouchers were selected from the rest of the participants.

The Google Play Console shows that 762 Android users installed CyberPal. Only 645 users participated in the study and these were randomly assigned to one of the nine groups. After reviewing the received responses, we eliminated 169 participants who either did not complete the pre- and/or, post-questionnaires. Moreover, 6 participants who completed both questionnaires either did not use the CyberPal app itself or were already using a password manager. After discarding these responses, 470 participants were retained to support analysis.

Variables and Measurement Units: In this experiment, the main variables were:

Independent variable: "*Intervention application that supports users' autonomy, competence and relatedness needs, in a variety of combinations*".

Dependent variable: "*Install a password manager*". This was measured by detecting if any password manager was installed on the participant's device within a week of using CyberPal. This was detected by regularly retrieving the names of all the applications on the user's device and checking whether a password manager appeared.

Control variable: "*Intention to use a password manager*". This was measured using instruments adapted from [46]. Self-reported responses were recorded on a 7 item Likert scale: seven means high intention to use a password manager, and 1 indicates low intention.

5. Analysis

62.8% of participants were male, 35.6% female. The majority were under 45 years of age. Inferential statistical tests were conducted using SPSS version 24 to test the hypotheses (Section 3).

Table 2 shows that the mean values of intention are relatively similar across groups; although it is slightly lower in Group 3. The sample size in each group is slightly different, an inevitable side effect of random allocation in the wild. To test the hypotheses, the analysis comprises two stages.

First, comparison between Group 1 and Group 9 to test hypotheses $H_a(0,1)$.

Second, comparison between the eight groups to test hypotheses $H_b(0,1\text{-}7)$.

Table 2. Descriptive Analysis (PM=Password Manager)

Grp	Sample Size	Intention Mean	Installed PM	Gender (F/M)
G1	43	4.60	1	(11/32)
G2	53	4.58	19	(14/38)
G3	52	4.14	9	(24/27)
G4	53	4.63	20	(21/31)
G5	51	4.62	18	(15/36)
G6	55	4.62	21	(20/33)
G7	54	4.36	18	(17/37)
G8	57	4.57	24	(22/34)
G9	52	4.57	9	(19/32)

Testing the Impact of the Recommender Application: A Crosstabulation test was carried out between G1 ('*the Placebo Group*') and G9 ('*the group with only the recommender system*').

The adoption rates were compared (the "*installing password manager*" variable). The latter was recorded as '1' for adoption, and '0' for non-adoption. A χ^2 test was conducted to determine whether there were significant differences in adoption behavior amongst participants in the two groups. The χ^2 statistic is 5.609. The the two-sided p-value is .018; which is significant at p $< .05$. It suggests that there are significant differences between the recommender system users, as compared to the group that merely enhanced awareness. Thus, the null hypothesis (H_a0) can be rejected. The alternative hypothesis was tested by comparing the means of password manager adoption in the two groups. Based on the result of the Crosstabulation test, the alternative hypothesis is accepted (H_a1).

Testing the Impact of SDT Need Satisfaction: Table 3 shows that when the three needs are satisfied (G8), more participants adopted password managers than participants in the other groups. This is followed by the case when Autonomy and Relatedness needs are met (G6).

We next needed to determine which factors exercised the greatest influence. First, three variables A, C, and R that represent the three needs were added to the data set. The presence of each need was coded as '1' while the absence was coded as '0'. To test the effect of autonomy, competence and relatedness need satisfaction on short-term adoption, a binary logistic regression test was conducted. It is important to note that the intention level is a strong predictor of adoption behavior [48]. Therefore, it was added as a control variable. As Table 3 shows, only relatedness and autonomy significantly influenced the adoption rate. Although the competence variable increased adoption, this effect is not significant. Moreover, the interactions between the three variables do not have a significant effect on adoption. To test the null hypothesis, that there is no difference between the eight groups with respect to password manager adoption rate, χ^2 tests were used. The null hypothesis (H_b0) can be rejected.

Table 3. Binary Logistic Regression (A=Autonomy, C=Competence, R=Relatedness) Significance Starred

Variables	β	**Std. Err.**	p
Intention	.915	.110	**.000***
A	1.099	.511	**.031***
C	.285	.562	.613
R	1.046	.514	**.042***
A*C	-.218	.723	.763
A*R	-.956	.685	.163
C*R	-.216	.732	.768
A*C*R	.423	.965	.661

Table 4. Hypothesis Summary (A*=Accepted* , R=Rejected)

H_a0	H_a1
R	***A****

H_b0	H_b1	H_b2	H_b3	H_b4	H_b5	H_b6	H_b7
R	***A****	R	***A****	R	R	R	R

Reasons for Adoption Decision: To understand why our participants chose, or did not choose, to install a password manager, we presented a post-questionnaire that popped up a week after they installed the app. We asked: "*Have you installed a password manager?*", with predefined multiple choice answers.

Of the 470 participants, 70% reported not installing a password manager while 30% did install one. Of those who installed, 81%(113) used it and 19%(26) had installed but not yet used it. The three top reasons for installing were that they could not remember their passwords (90%), to store their data securely (53%), and to keep passwords synchronized across devices (37%). Top reasons for NOT installing included the fact that it took too much time to set up (30%), trust issues (30%) and external factors such as a lack of storage space (8%).

6. Discussion

This study empirically tested the impact of an intervention that satisfied participants' SDT needs, and then observed their actions in terms of installing a password manager. We experimentally manipulated autonomy, competence, and relatedness need satisfaction within the context of recommending a password manager to determine which of the individual needs, or which combination thereof, exerted the most powerful influence.

This intervention enabled an effective test of SDT's assumption that SDT's autonomy, competence and relatedness need satisfaction yield positive behavioral outcomes. Based on SDT's predictions, we would expect all three to impact on adoption. Our study showed that autonomy and relatedness need satisfaction did indeed have a significant impact on adoption decisions.

Furthermore, although SDT only predicts the additive relations between the factors and the performance of the target behavior, we were interested in exploring the effect of two- and three-way interactions between the factors. We did not detect significant interaction effects.

Recommendations: This study offers useful insights into the potential of applying SDT and recommender systems to support the search for a suitable password manager. As already mentioned, the study provided evidence of the positive impact of supporting autonomy and relatedness needs. Doing this makes it more likely that Android Smartphone users will adopt a password manager.

Adoption Intervention: When giving security advice to end users, it is important to make it possible for them to consider the adoption decision from a personal perspective. A previous study [8] found that after a user becomes aware of password managers, and planned to use one, they would commence the process by searching for a suitable one. If they decided to proceed, a selection would be made from the proffered options. Supporting the user's search and decide decisions, by providing a recommender system, facilitates behavioral adaptations i.e. *trials*.

This mechanism might be applied to improve adoption of other security tools by providing appropriate interventions to facilitate the adoption process.

Furthermore, the nexus between SDT and the awareness intervention provided by the recommender app is an important contribution.

Relatedness: Some password manager providers already use word-of-mouth referrals by encouraging their users to invite other potential users. Our study provides evidence of the effectiveness of such referral systems in encouraging adoption. Our way of supporting relatedness does not undermine the users' autonomy need by mandating one particular password manager. Instead, it engaged the users in the decision-making process and makes suggestions in line with the user's own preferences.

Autonomy: Employing non-controlling language and providing choices to support autonomy successfully encouraged more users to adopt a password manager. Using bossy language when advising the users to improve their security might violate autonomy. For example, instructing users with: "*you have to change your password!*" might lead to a reactance response. As already noted, providing choice concerning a difficult decision, such as choosing a password manager application, supports the autonomy need. This might explain why Fagan *et al.* [69] found, in their study, that participants preferred the software update/warning message design that gave them different update options.

Competence: Unexpectedly, the effect of Competence was not significant. However, we cannot conclude from our study that the satisfaction of competence will always be insignificant. Two explanations suggest themselves for our results. The *first* is that the way we satisfied competence might have been suboptimal and did not genuinely meet the person's competence needs. The *second* is that this particular group happened to contain more low intention participants than others, purely by chance.

Furthermore, competence might be less effective with critical systems. Bonini [70] found that the manipulation of competence did not have a significant effect on air traffic controllers' decisions to trust other controllers or their technology.

Another possible explanation is the fact that competence takes time to acquire [71]. Our study was a short-term experiment and, given the criticality of the data, it might be that more time is needed to develop competence. Finally, electronic recommendations might create more uncertainty than face-to-face interaction with an expert [72], by exacerbating feelings of uncertainty.

Reasons for the adoption decision: Although the main function of a password manager is to provide a solution to password security and memorability issues, the analysis of the post questionnaire revealed that a majority of users adopted password managers to support their memory. The study also found that one of the barriers for not installing a password manger is the time it takes to set it up. Developers need to minimize password manager setup times. Moreover, the popularity of password managers among small groups of users can convince more users to adopt these tools.

Summary: Security system designers should consider supporting autonomy, relatedness and competence needs when designing their system interfaces. Moreover, we should pay attention to supporting the recommended security behavior from the user's perspective.

Study Limitations: ***First***, given that the study was conducted in the wild, we were not able to ensure that participants paid attention to the language used by the recommender application. ***Second***, we did not conduct manipulation checks to ensure that the variations in the design had their intended effects [73]. We included a FAQ feature to satisfy the competence need, but we do not know that it actually did so. Nevertheless, according to O'Keefe [74], when message variations are identified in terms of intrinsic features, manipulation checks are unnecessary. ***Third***, since the study encouraged participants to recruit other participants in order to support the relatedness need, this might have led to a sampling bias. ***Fourth***, in-the-wild studies make it impossible to control all external variables. It is possible that factors such as limited storage or time pressure, for example, prevented adoption. ***Finally***, we verified whether or not the participants had installed a password manager. This does not mean that they necessarily retained it. A study to monitor usage longitudinally would deliver more reliable insights into long-term adoption.

7. Conclusions & Future Work

Very few people use these password managers, and we wanted to determine whether we could encourage adoption by meeting people's self determination needs. We ran a longitudinal experiment, offering people a recommender application that met their needs, and monitored their device to see whether they subsequently installed a password manager. We discovered that satisfying the three needs, particularly autonomy and relatedness, did indeed encourage adoption.

The next step is to explore the factors affecting the long-term adoption. However, we first need to focus more closely on meeting competence needs,to find ways of satisfying this need more effectively.

References

[1] Y. Li, H. Wang, and K. Sun, "A study of personal information in human-chosen passwords and its security implications," in *INFOCOM 2016*, 2016, pp. 1–9.

[2] S. Furnell and R. Esmael, "Evaluating the effect of guidance and feedback upon password compliance," *Computer Fraud & Security*, vol. 2017, no. 1, pp. 5–10, 2017.

[3] K. K. Greene and Y.-Y. Choong, "Must I, can I? I don't understand your ambiguous password rules," *Information & Computer Security*, vol. 25, no. 1, pp. 80–99, 2017.

[4] S. M. Segreti, W. Melicher, S. Komanduri, D. Melicher, R. Shay, B. Ur, L. Bauer, N. Christin, L. F. Cranor, and M. L. Mazurek, "Diversify to survive: Making passwords stronger with adaptive policies," in *SOUPS*, 2017.

[5] K. Renaud, "Blaming noncompliance is too convenient: What really causes information breaches?" *IEEE Security & Privacy*, vol. 10, no. 3, pp. 57–63, 2012.

[6] B. Korbar, J. Blythe, R. Koppel, V. Kothari, and S. W. Smith, "Validating an agent-based model of human password behavior." in *AAAI Workshop: Artificial Intelligence for Cyber Security*, 2016.

[7] Roboform.com, "Password manager," 2016 (accessed January 10, 2018), https://www.roboform.com/password-manager.

[8] N. Alkaldi and K. Renaud, "Why do people adopt, or reject, smartphone password managers?" in *EuroUSEC*, 2016.

[9] A. A. Al-Daraiseh, D. Al Omari, H. Al Hamid, N. Hamad, and R. Althemali, "Effectiveness of iPhones Touch ID: KSA case study," *Editorial Preface*, vol. 6, no. 1, 2015.

[10] M. Bada and A. Sasse, *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* Global Cyber Security Capacity Centre, University of Oxford, 2014.

[11] R. M. Ryan and E. L. Deci, “Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being.” *American Psychologist*, vol. 55, no. 1, p. 68, 2000.

[12] K. Renaud and V. Zimmermann, “Nudging folks towards stronger password choices: providing certainty is the key,” *Behavioural Public Policy*, pp. 1–31, February 2018.

[13] R. Biddle, S. Chiasson, and P. C. van Oorschot, “Graphical passwords: Learning from the first twelve years,” *ACM Computing Surveys*, vol. 44, pp. 19:1–19:41, 2012.

[14] E. G. Agulla, L. A. Rifón, J. L. A. Castro, and C. G. Mateo, “Is my student at the other side? Applying biometric web authentication to e-learning environments,” in *ICALT’08*, 2008, pp. 551–553.

[15] N. Gunson, D. Marshall, H. Morton, and M. Jack, “User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking,” *Computers & Security*, vol. 30, no. 4, pp. 208–220, 2011.

[16] R. Ahuja, M. Ramrakhyani, B. Manchundiya, and S. Shroff, “Dual Layer Secured Password Manager using Blowfish and LSB,” *International Journal of Computer Applications*, vol. 143, no. 3, 2016.

[17] L. Wang, Y. Li, and K. Sun, “Amnesia: A bilateral generative password manager,” in *ICDCS*, 2016, pp. 313–322.

[18] J. Gray, V. N. Franqueira, and Y. Yu, “Forensically-sound analysis of security risks of using local password managers,” in *Requirements Engineering Conference Workshops (REW)*, 2016, pp. 114–121.

[19] R. Zhao, C. Yue, and K. Sun, “Vulnerability and risk analysis of two commercial browser and cloud based password managers,” *ASE Science Journal*, vol. 1, no. 4, pp. 1–15, 2013.

[20] N. M. Barbosa, J. Hayes, and Y. Wang, “Unipass: design and evaluation of a smart device-based password manager for visually impaired users,” in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2016, pp. 49–60.

[21] S. Chiasson, P. C. van Oorschot, and R. Biddle, “A usability study and critique of two password managers.” in *USENIX Security Symposium*, 2006, pp. 1–16.

[22] A. Karole, N. Saxena, and N. Christin, “A comparative usability evaluation of traditional password managers,” in *International Conference on Information Security and Cryptology*, Seoul, Korea, 2010, pp. 233–251.

[23] A. Whitten and J. Tygar, “Why Johnny can’t encrypt: a usability evaluation of PGP 5.0,” in *Proceedings of the 8th conference on USENIX Security Symposium-Volume 8*, 1999.

[24] A. Beautement, M. A. Sasse, and M. Wonham, “The compliance budget: managing security behaviour in organisations,” in *NSPW*, 2008, pp. 47–58.

[25] K. Renaud, M. Volkamer, and A. Renkema-Padmos, “Why doesn’t Jane protect her privacy?” in *PETS*, 2014, pp. 244–262.

[26] M. Fagan and M. M. H. Khan, “Why do they do what they do?: A study of what motivates users to (not) follow computer security advice,” in *SOUPS*, 2016, pp. 59–75.

[27] A. Beautement and A. Sasse, “The economics of user effort in information security,” *Computer Fraud & Security*, vol. 2009, no. 10, pp. 8–12, 2009.

[28] C. Herley, “So long, and no thanks for the externalities: the rational rejection of security advice by users,” in *NSPW*, 2009, pp. 133–144.

[29] R. M. Ryan and E. L. Deci, “Intrinsic and extrinsic motivations: Classic definitions and new directions,” *Contemporary Educational Psychology*, vol. 25, no. 1, pp. 54–67, 2000.

[30] E. Deci and R. Ryan, *Intrinsic Motivation and Self-Determination in Human Behavior*, ser. Perspectives in Social Psychology. Rochester, New York: Kluwer, 1985.

[31] W.-T. Wang and Y.-P. Hou, “Motivations of employees’ knowledge sharing behaviors: A self-determination perspective,” *Information and Organization*, vol. 25, no. 1, pp. 1–26, 2015.

[32] C. R. France, J. L. France, B. W. Carlson, V. Frye, L. Duffy, D. A. Kessler, M. Rebosa, and B. H. Shaz, “Applying self-determination theory to the blood donation context: The blood donor competence, autonomy, and relatedness enhancement (Blood Donor CARE) trial,” *Contemporary Clinical Trials*, vol. 53, pp. 44–51, 2017.

[33] Y. Chen, K. Ramamurthy, and K.-W. Wen, “Organizations’ information security policy compliance: Stick or carrot approach?” *Journal of Management Information Systems*, vol. 29, no. 3, pp. 157–188, 2012.

[34] J. C. Siemens, S. Smith, D. Fisher, A. Thyroff, and G. Killian, “Level up! The role of progress feedback type for encouraging intrinsic motivation and positive brand attitudes in public versus private gaming contexts,” *Journal of Interactive Marketing*, vol. 32, pp. 1–12, 2015.

[35] A. AlMarshedi, G. B. Wills, and A. Ranchhod, “The Wheel of Sukr: a framework for gamifying diabetes self-management in Saudi Arabia,” *Procedia Computer Science*, vol. 63, pp. 475–480, 2015.

[36] D. H. Pink, *Drive: The surprising truth about what motivates us.* Edinburgh, U.K.: Penguin, 2011.

[37] K. Kreijns, M. Vermeulen, F. Van Acker, and H. van Buuren, “Predicting teachers’ use of digital learning materials: combining self-determination theory and the integrative model of behaviour prediction,” *European Journal of Teacher Education*, vol. 37, no. 4, pp. 465–478, 2014.

[38] G. C. Williams, H. Patrick, C. P. Niemiec, R. M. Ryan, E. L. Deci, and H. M. Lavigne, “The smoker’s health project: a self-determination theory intervention to facilitate maintenance of tobacco abstinence,” *Contemporary Clinical Trials*, vol. 32, no. 4, pp. 535–543, 2011.

[39] P. Menard, G. J. Bott, and R. E. Crossler, “User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory,” *Journal of Management Information Systems*, vol. 34, no. 4, pp. 1203–1230, 2017.

[40] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, “Are you ready to lock?” in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 750–761.

[41] T. F. Van de Mortel, “Faking it: social desirability response bias in self-report research,” *The Australian Journal of Advanced Nursing*, vol. 25, no. 4, p. 40, 2008.

[42] S. Ruoti, J. Andersen, S. Heidbrink, M. O’Neill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons, “We’re on the same page: A usability study of secure email using pairs of novice users,” in *CHI*, 2016, pp. 4298–4308.

[43] D. Machuletz, H. Sendt, S. Laube, and R. Böhme, "Users Protect Their Privacy If They Can: Determinants of Webcam Covering Behavior," in *EuroUSEC*, 2016.

[44] S. Egelman, M. Harbach, and E. Peer, "Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS)," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, San Jose, USA, 2016, pp. 5257–5261.

[45] S. Aurigemma, T. Mattson, and L. Leonard, "So much promise, so little use: What is stopping home end-users from using password manager applications?" in *HICSS*, 2017.

[46] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Computers & Security*, vol. 49, pp. 177–191, 2015.

[47] M. N. Silva, M. M. Marques, and P. J. Teixeira, "Testing theory in practice: The example of self-determination theory-based interventions," *European Health Psychologist*, vol. 16, no. 5, pp. 171–180, 2014.

[48] T. Gugathas, "How to develop physical activity programs for elderly to facilitate their motivation to follow physical activity recommendations? A Social Determination Theory-based approach," Master's thesis, University of Twente, 2016.

[49] J. C. Sweeney, D. Webb, T. Mazzarol, and G. N. Soutar, "Self-determination theory and word of mouth about energy-saving behaviors: an online experiment," *Psychology & Marketing*, vol. 31, no. 9, pp. 698–716, 2014.

[50] J. L. Szalma, "On the application of motivation theory to human factors/ergonomics: Motivational design principles for human–technology interaction," *Human Factors*, vol. 56, no. 8, pp. 1453–1471, 2014.

[51] A. Wiklund-Engblom, M. Hassenzahl, A. Bengs, and S. Sperring, "What needs tell us about user experience," in *IFIP Conference on Human-Computer Interaction*, Uppsala, Sweden, 2009, pp. 666–669.

[52] D. N. Stone, E. L. Deci, and R. M. Ryan, "Beyond talk: Creating autonomous motivation through self-determination theory," *Journal of General Management*, vol. 34, no. 3, pp. 75–91, 2009.

[53] Y.-L. Su and J. Reeve, "A meta-analysis of the effectiveness of intervention programs designed to support autonomy," *Educational Psychology Review*, vol. 23, no. 1, pp. 159–188, 2011.

[54] J. Reeve, "Autonomy-supportive teaching: What it is, how to do it," in *Building Autonomous Learners*. Springer, 2016, pp. 129–152.

[55] S. Maxwell, "Hyperchoice and high prices: an unfair combination," *Journal of Product & Brand Management*, vol. 14, no. 7, pp. 448–454, 2005.

[56] R. G. Straton and R. M. Catts, "A comparison of two, three and four-choice item tests given a fixed total number of choices," *Educational and Psychological Measurement*, vol. 40, no. 2, pp. 357–365, 1980.

[57] S. M. Andersen, S. Chen, and C. Carter, "Fundamental human needs: Making social cognition relevant," *Psychological Inquiry*, vol. 11, no. 4, pp. 269–275, 2000.

[58] A. Hassan, "Managing Students Motivation: an Empirical Study from Seld-Determination Perspective," in *ICMIP-2 2014*, 2014.

[59] H. P. Young, "Innovation diffusion in heterogeneous populations: Contagion, social influence, and social learning," *American Economic Review*, vol. 99, no. 5, pp. 1899–1924, 2009.

[60] A. Bakx, T. Van Houtert, M. v. d. Brand, and L. Hornstra, "A comparison of high-ability pupils' views *vs.* regular ability pupils' views of characteristics of good primary school teachers," *Educational Studies*, pp. 1–22, 2017.

[61] J. M. Harackiewicz, G. Manderlink, and C. Sansone, "Rewarding pinball wizardry: Effects of evaluation and cue value on intrinsic interest." *Journal of Personality and Social Psychology*, vol. 47, no. 2, p. 287, 1984.

[62] L. Jussim, S. Soffin, R. Brown, J. Ley, and K. Kohlhepp, "Understanding reactions to feedback by integrating ideas from symbolic interactionism and cognitive evaluation theory." *Journal of Personality and Social Psychology*, vol. 62, no. 3, p. 402, 1992.

[63] E. M. Thuen, "Learning environment, students' coping styles and emotional and behavioural problems," Ph.D. dissertation, Department of Psycosocial Science, Faculty of Psychology, The University of Bergen, 2007.

[64] International Data Corporation (IDC Corporate USA), "Smartphone OS Market Share, 2017 Q1," 2018 (accessed January 10, 2018), https://www.idc.com/promo/smartphone-market-share/os.

[65] E. Kim, "The meteoric rise of iOS and Android in one chart," 2016 (accessed January 10, 2018), http://uk.businessinsider.com/ios-and-android-dominate-marketshare-2016-2?r=US&IR=T.

[66] R. Rosenthal and R. L. Rosnow, *Artifacts in behavioral research: Robert Rosenthal and Ralph L. Rosnow's classic books*. New York, USA: Oxford University Press, 2009.

[67] B. Shiv, Z. Carmon, and D. Ariely, "Placebo effects of marketing actions: Consumers may get what they pay for," *Journal of Marketing Research*, vol. 42, no. 4, pp. 383–393, 2005.

[68] F. G. Miller, L. Colloca, and T. J. Kaptchuk, "The placebo effect: illness and interpersonal healing," *Perspectives in Biology and Medicine*, vol. 52, no. 4, p. 518, 2009.

[69] M. Fagan, M. M. H. Khan, and N. Nguyen, "How does this message make you feel? A study of user perspectives on software update/warning message design," *Human-Centric Computing and Information Sciences*, vol. 5, no. 1, p. 36, 2015.

[70] A. Brodje, M. Lundh, J. Jenvald, and J. Dahlman, "Exploring non-technical miscommunication in vessel traffic service operation," *Cognition, Technology & Work*, vol. 15, no. 3, pp. 347–357, 2013.

[71] J. G. March, "The future, disposable organizations and the rigidities of imagination," *Organization*, vol. 2, no. 3-4, pp. 427–440, 1995.

[72] S. I. Shim and Y. Lee, "Consumer's perceived risk reduction by 3D virtual model," *International Journal of Retail & Distribution Management*, vol. 39, no. 12, pp. 945–959, 2011.

[73] K. Marett, "Checking the manipulation checks in information security research," *Information & Computer Security*, vol. 23, no. 1, pp. 20–30, 2015.

[74] D. J. O'Keefe, "Message properties, mediating states, and manipulation checks: Claims, evidence, and data analysis in experimental persuasive message effects research," *Communication Theory*, vol. 13, no. 3, pp. 251–274, 2003.