



University
of Glasgow

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

<https://theses.gla.ac.uk/74359/>

Copyright and moral rights for this work are retained by the author

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

This work cannot be reproduced or quoted extensively from without first obtaining permission from the author

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given

Enlighten: Theses

<https://theses.gla.ac.uk/>
research-enlighten@glasgow.ac.uk

Adopting Password Manager Applications among Smartphone Users

Nora Abdullah Alkaldi

Submitted in fulfilment of the requirements for the
Degree of Doctor of Philosophy

School of Computing Science
College of Science and Engineering
University of Glasgow



University
of Glasgow

March 2019

Abstract

People use weak passwords for a variety of reasons, the most prescient of these being memory load and inconvenience. The motivation to choose weak passwords is even more compelling on smartphones because entering complex passwords is particularly time consuming and arduous on small devices. Password managers are a potential solution to the password conundrum, but it is unfortunate that these applications have not enjoyed widespread adoption.

This thesis investigated the adoption of password manager applications and filled an important gap in the human-centric and information security literature. It concentrated on end users' perceptions, the factors that influence the adoption decisions of password managers and how to encourage them to adopt these tools.

The thesis begins with an exploratory study to investigate the current state of password manager adoption and to understand the reasons that impede or encourage the adoption of password managers. Qualitative data was collected and the data was analysed using Grounded Theory. This study found that the adoption process of password managers goes through six stages. Accordingly, recommendations were suggested to improve the adoption of password manager applications.

The factors that influence the intention to adopt a password manager were next identified and empirically validated using migration theory as a theoretical foundation. These factors were identified based on interviews with smartphone users, resulting in a proposed migration model. The proposed model was then tested quantitatively with smartphone users. Structural Equation Model (SEM) analysis found that users' dissatisfaction with their password-coping behaviours, and their perception of the usefulness and the effectiveness of password managers positively influenced their intention to adopt a password manager. On the other hand, users' perceived risk of using password managers, and the cost of setting up these tools, deterred the intention to adopt. Also, the result confirmed the positive influence of social influence (Descriptive norms) on adoption intention.

Finally, the thesis presents an investigation into the impact of a recommender application that

harnessed the tenets of self-determination theory to encourage the 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, a factorial experiment was conducted, in the wild. Each of the three self-determination factors and all individual combinations thereof were satisfied, and the short-term adoption of password managers was observed (i.e. the installation of a password manager). When all the self-determination factors were satisfied, adoption was highest, while meeting only the autonomy or relatedness needs individually significantly improved the likelihood of adoption.

Contents

Abstract	i
Acknowledgements	x
Declaration	xi
List of Publications	xii
Acronyms	xiii
1 Introduction	1
1.1 Research Overview and Motivation	1
1.2 Research Aims and Objectives	3
1.3 Research Contribution	4
1.4 Overview of the Thesis	5
2 Literature Review	7
2.1 Introduction	7
2.2 Knowledge-based Authentication	7
2.3 Text-based Passwords	8
2.4 Password Problems	8
2.5 Users' Password-related Behaviours	10
2.5.1 Password usage	10
2.5.2 Creating passwords	12
2.5.3 Changing passwords	18
2.5.4 Reusing passwords	19
2.5.5 Recording passwords	20
2.5.6 Sharing passwords	21
2.5.7 Summary	22
2.6 Schemes to improve Text-based Passwords	22
2.6.1 System-generated passwords	22
2.6.2 Enhancing user-generated passwords	23

2.6.3	Password instructions at creation time	23
2.6.4	Mnemonic strategy	24
2.6.5	Password cue	25
2.6.6	Password-creation feedback	26
2.6.7	Password policy	28
2.6.8	Password chunking	30
2.7	Other Approaches to the Password Problem	31
2.7.1	Single-sign-on	31
2.7.2	Token-based authentication	31
2.7.3	Biometric authentication	32
2.7.4	Two-factor authentication	33
2.7.5	Graphical password	33
2.8	Password Management Systems	35
2.8.1	Additional features of password managers	35
2.8.2	Types of password managers	37
2.8.3	Adoption of password managers	38
2.8.4	Password-manager-related works	39
2.9	Conclusion	41
3	Password Manager Adaption Stages: An Exploratory Investigation Study	42
3.1	Introduction	42
3.2	Study Approach	43
3.3	Data Collection	43
3.4	Qualitative Analysis	45
3.4.1	Open Coding	45
3.4.2	Axial Coding	46
3.4.3	Selective Coding	63
3.4.4	Password Manager Adoption Lifecycle	64
3.5	Adoption Example	65
3.6	Discussion	66
3.7	Conclusion	70
4	Theoretical Background	71
4.1	Introduction	71
4.2	Theoretical Model for Predicting Behaviour Intention	71
4.3	Measuring Actual Information Security Behaviour	73
4.4	Recommendation Systems	74
4.5	Motivational Theories	76
4.6	Conclusion	81

5	Adopting Password Manager: A Migration Theoretic Analysis	82
5.1	Introduction	82
5.2	Theoretical Model	82
5.3	Eliciting Study (Semi-structured Interview)	84
5.4	Password manager Migration Model	88
5.4.1	Pull Factors	88
5.4.2	Push Factors	88
5.4.3	Mooring Factors	89
5.4.4	Other Factors	90
5.4.5	Intention and Actual Adoption	90
5.5	Methodology	91
5.5.1	Study Design	91
5.5.2	Measurement	91
5.5.3	Data Collection	96
5.6	Data Analysis and Results	96
5.6.1	Data Screening	97
5.6.2	Descriptive Analysis	100
5.6.3	Measurement Model	101
5.6.4	Structural Model	107
5.7	Discussion	115
5.8	Conclusion	119
6	Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs	121
6.1	Introduction	121
6.2	Study Aims and Hypotheses	121
6.2.1	The Impact of the Recommender System	122
6.2.2	The Impact of Needs Satisfaction	122
6.3	Intervention Design	123
6.3.1	Raising Awareness	123
6.3.2	The CyberPal Recommender Application	123
6.3.3	Behavioural Intention	134
6.3.4	Testing	135
6.4	Data Collection	135
6.4.1	Experiment Design	135
6.4.2	Ethical Considerations	137
6.4.3	Task	137
6.4.4	Recruitment	138
6.4.5	Variables and Measurement Units	138

6.5	Analysis	139
6.5.1	Testing the Impact of the Recommender Application	142
6.5.2	Testing the Impact of SDT Need Satisfaction	143
6.5.3	Reasons for Adoption Decision	144
6.5.4	Password Manager Features	145
6.6	Discussion	147
6.7	Conclusion	152
7	Discussion and Implications	153
7.1	Introduction	153
7.2	How Do Users Adopt a Password Manager?	153
7.3	What Are the Factors That Inform Users' Intentions to Adopt a Password Manager?	154
7.4	The Need for Adoption Support	154
7.5	The Power of SDT in Adopting Password Managers	155
7.6	Implications	156
7.7	Conclusion	158
8	Conclusion	160
8.1	Thesis Summary	160
8.2	Contributions	161
8.3	Limitations	162
8.4	Future Research Directions	163
A	Online Survey	165
A.1	Survey Questionnaire	165
A.2	Participant Consent Form	166
A.3	Ethical Approval	167
B	Interview Study	168
B.1	Questionnaire Script	168
B.1.1	Demographic Data	168
B.1.2	Smartphone Usage and Password Experience	169
B.1.3	Password Manager	170
B.2	Participant Consent Form	171
B.3	Ethical Approval	172
C	Experiment	173
C.1	Password Manager Features	173
C.2	Pre questionnaire	174

C.3	Post questionnaire	180
C.4	Participant Consent Form	183
C.5	Ethical Approval	184
Bibliography		185

List of Tables

3.1	The codes used in the open coding stage grouped by the initial axial coding categories	47
3.2	Some of the main functionalities of Password Manager	59
3.3	The final axial coding	63
5.1	Security behaviour studies	83
5.2	Factors affecting users' decision to adopt a password manager	85
5.3	Push, Pull and Moor factors	87
5.4	Measurement item descriptions	91
5.5	Descriptive statistics	98
5.6	Correlation Matrixes	99
5.7	Variance inflation factor	100
5.8	Descriptive Data	101
5.9	Standardized Regression Weights	102
5.10	Average variance extracted for validity testing	104
5.11	Constructs' Reliability	105
5.12	Discriminant validity	106
5.13	Model Fit Indices cut-off values	107
5.14	Summary of overall measurement model	107
5.15	Structural equation model results	109
5.16	Hypothesis testing results	115
6.1	Supporting Self Determination Needs in CyberPal app	134
6.2	Description of the experimental groups	136
6.3	Descriptive Analysis	142
6.4	Binary Logistic Regression	143
6.5	Reasons for installing a password manager	144
6.6	Reasons for not installing a Password Manager	145
6.7	The selected features in CyberPal	146

List of Figures

3.1	Arranging the codes in the axial coding process	47
3.2	Password manager adoption stages	65
4.1	Migration Theory	73
5.1	The proposed conceptual model with hypothesis	108
5.2	Hypothesis testing results	114
5.3	Password manager migration final model	119
6.1	Password manager features in CyberPal	128
6.2	Order preferences	129
6.3	Supporting autonomy in the recommender app	130
6.4	Supporting relatedness in the recommender app	131
6.5	Supporting relatedness-who use a password manager in your contact	132
6.6	Supporting competences in the recommender app	133
6.7	Group 1-placebo interface	137
6.8	Participants' demographics	139
6.9	Participants' education level	140
6.10	Participants' methods for managing their passwords	140
6.11	Participants' awareness of password manager	141
6.12	Participants' IT skill level	141
6.13	Participants' information security knowledge	142
6.14	Respondent's rating of the features of password manager applications	147

Acknowledgements

I would like to thank my supervisors Prof. Karen Renaud and Dr. Lewis Mackenzie for their excellent advice, productive meetings, unlimited support, and guidance throughout my PhD journey. Their immense knowledge, insightful comments, suggestions and feedback helped me to shape my research ideas. For that, I will be forever thankful.

I am thankful to the University of Glasgow for providing the best research facilities and support services to complete my research.

I would like also to express my appreciation to all staff and students at the School of Computing Science for their help and support during my years at the university.

I am grateful to my sponsors (King Saud University) for granting me the scholarship and the opportunity to achieve one of my dreams.

I take this opportunity to express my profound gratitude to my beloved parents, Abdullah and Sarah, and my wonderful husband Mohammed for their patience, endless support, unconditional love and prayers during my study. Heartfelt thanks goes to my amazing siblings, family and friends for their encouragement and support.

Finally I owe special thanks to my children Ameerah, Hassah and Omar for their patience and understanding throughout the research and writing of the thesis. Their kind wishes were great source of motivation for the successful completion of this research.

Declaration

I certify that the thesis presented here for examination for PhD degree of the University of Glasgow is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it) and that the thesis has not been edited by a third party beyond what is permitted by the University's PGR Code of Practice.

The copyright of this thesis rests with the author. No quotation from it is permitted without full acknowledgment.

I declare that the thesis does not include work forming part of a thesis presented successfully for another degree (unless explicitly identified and as noted below). I declare that this thesis has been produced in accordance with the University of Glasgow's Code of Good Practice in Research.

I acknowledge that if any issue are raised regarding good research practice based on review of the thesis, the examination may be postponed pending the outcome of any investigation of the issues.

Nora Alkaldi

March 2019

List of Publications

1. Alkaldi, N & Renaud, K 2016, Why do people adopt, or reject, smartphone password managers? in EuroUSEC '16: the 1st European Workshop on Usable Security. Internet Society, Darmstadt, 1st European Workshop on Usable Security, volume 18, pages 1-14, Darmstadt, Germany, 18/07/16.
<https://doi.org/10.14722/eurosec.2016.23011>
2. Alkaldi, N & Renaud, K 2016, Why do people adopt, or reject, smartphone security tools? in NL Clarke & SM Furnell (eds), Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016. Univerisity of Plymouth, Plymouth, pp. 135-144, 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016, Frankfurt, Germany, 19-21/07/16.
3. Alkaldi, N, Renaud, K & Mackenzie, L 2019, Encouraging password manager adoption by meeting adopter self-determination needs. In Proceedings of the 52nd Hawaii International Conference on System Sciences. University of Hawaii at Manoa, pp. 4824-4833, Hawaii International Conference on System Sciences, United States, 8/01/19.
<https://doi.org/10.1255/59920>

Acronyms

- **PM:** Password Manager
- **HACK :** Exposure to Hacking
- **PWMSEC:** Security Concerns
- **PRISK:** Perceived Risk
- **PWMPRIV:** Privacy Concerns
- **INT:** Intention
- **PWMFEE:** Monetary Cost
- **PWMSETC:** Set-up Cost
- **PWMLC:** Learning Cost
- **RCMAN:** Response Cost of Managing Passwords
- **RU:** Relative Usefulness
- **PWMREFF:** PM Response Efficacy
- **INNOV:** Innovativeness
- **DNORM:** Descriptive Norm
- **DISSAT:** Dissatisfaction
- **PVUL:** Perceived Vulnerability
- **TRA :** Theory of Reasoned Action
- **TAM :** Technology Acceptance Model
- **TPB:** Theory of Planned Behaviour
- **SCT:** Social Cognitive Theory

- **PMT:** Protection Motivation Theory
- **HBM :** Health Belief model
- **GDT:** General Deterrence Theory
- **SDT :** Self-Determination Theory
- **SSO :** Single Sign-On
- **TBA:** Token-Based Authentication
- **OTP:** One-Time Password
- **2FA:** Two-Factor Authentication
- **SNS:** Social Networking Services
- **MTurk:** Amazon's Mechanical Turk crowdsourcing service
- **SEM:** Structural Equation Modelling
- **VIF:** Variance Inflation Factor
- **CFA:** Confirmatory Factor Analysis
- **AVE:** Average Variance Extracted
- **CFI:** Comparative Fit Index
- **IFI:** Incremental Fit Index
- **TLI:** Turker-Lewis Index
- **REMSEA:** Root Mean Square Error of Approximation
- **CR:** Critical Ratio

Chapter 1

Introduction

Text-based passwords are still the dominant user authentication method for the majority of websites, from social networks, electronic stores and e-mails to banks. However, this method suffers from both security and usability problems. Password management applications are the best available solutions to the password problem. Despite existing research into password manager systems and a wide range of available managers, this tool is not widely adopted. There is also a lack of human-centric research into password managers and the adoption of these tools. Therefore, this research aims to investigate the adoption of password manager applications and it fills an important gap in the human-centric and information security literature. This chapter presents an overview of the research and identifies the research gap that motivated the research reported in this dissertation. Then, the aims and objectives of the research are provided, followed by a discussion of the research contribution. Finally, an overview of the thesis structure is provided to conclude this chapter.

1.1 Research Overview and Motivation

Passwords are considered the first line of defence on any computer device and network system. They present a crucial barrier between attackers and these devices and systems. Since passwords are usually chosen by end users, they often choose passwords that are weak, as users need to remember them with ease. Even when relatively strong passwords are generated by different applications, end users tend to reuse them or write them down, weakening again the security [1,2]. These password management behaviours make it easier for attackers to gain access to all sorts of accounts and systems. The password management for smartphone users might be even more critical due to design limitations in these devices such as screen size and keyboard multi-layer interaction. Typing secure long passwords with different types of character classes becomes tedious on these devices, increasing the use of weak passwords [3].

A password manager is a security tool that handles the password problems for users [4]. It

helps the user to generate secure passwords for each account and fills in the log in information automatically on behalf of the user. Thus, users do not need to remember their passwords or know which password is associated with which account. Password managers also help to protect against shoulder surfing, brute force and dictionary attacks [5]. However, this tool is not yet widely adopted by end users [2, 6]. The low adoption rate of password managers has been also reported for other security tools such as screen lock and anti-theft applications [7,8,9]. Usability has always been blamed for the poor adoption of security tools [10,1]. However, even usable technologies, such as fingerprint authentication, are not widely adopted [11].

There is increasing interest in applying behavioural interventions to trigger behavioural change. It has become commonplace in the health sector [21] and has recently been applied in other domains such as energy saving [12] and cybersecurity [18]. The exploratory study (Chapter 3) found that the adoption process of password manager goes through six stages: awareness, intention, searching, deciding, trying and long-term adoption. To encourage the adoption of password managers, a smartphone intervention is developed in a form of a password manager recommender system named "CyberPal". The app raises awareness of password managers and supports users in searching and deciding, then observes whether an initial trial ensues or not.

Researchers in other fields, such as psychology and marketing, have found that satisfying psychological basic needs can influence the adoption of certain behaviours [12,13,14]. In this regard, Self-Determination Theory (SDT) is a motivation theory that has been successfully applied in different contexts over 40 years, studying the effect of three psychological basic needs and their influence on human behaviour [15]. This theory assumes that satisfying the human psychological basic needs of autonomy, competency and relatedness can determine an individual's level of motivation for the behaviour of interest. Being interested in studying the adoption of password management tools, this research also aims to investigate whether satisfying the three basic needs proposed by the SDT would encourage smartphone users to adopt password manager applications. Therefore, an intervention was designed to support users' three basic needs in order to encourage the adoption of a password manager.

Studies on technology adoption and behaviour change have considered theoretical models to identify the significant factors that encourage adoption behaviour, such as the Technology Acceptance Model (TAM), for example [16], which has been widely used in the information system field. This may help to penetrate the reasons behind the low/high adoption of behaviours. Throughout the different studies applying theoretical models, some researchers applied models from other disciplines such as the Health Belief model (HBM) [17] from the health sector, the General Deterrence Theory (GDT) [18] from the crime and justice area and migration theory [19] from human geography literature. Migration theory [19], which explains migration deci-

sions based on push-pull and mooring effects, reflects a process of moving from one state to a new state. Unlike some of the technologies, where the adoption decision is independent, adopting a password manager involves switching from the current password management method to the use of a password manager tool. Therefore, applying migration theory to depict the factors that influence the intention to adopt a password manager seems a promising way to explore why end users would adopt, or not adopt, a password manager.

Little research has discussed the human side of password manager systems. The lack of human-centric studies of password managers has created a gap that needs filling. The advantages provided by the password manager, coupled with its low adoption rate and the lack of human-centric studies about it provided the motivation of this research into the adoption of password management applications. Thus, this research seeks to fill that gap by exploring end users' perceptions about adopting password managers and designing and testing an intervention to encourage the adoption of these tools.

1.2 Research Aims and Objectives

The primary aim of this research is to explore the current state of using password managers, find the significant behavioural antecedents of adopting these tools and experimentally determine whether applying self-determination factors in an intervention will have an impact on encouraging the subsequent adoption of password managers.

Hence, this research addresses the following research questions:

- Q1.** What is the current status of password manager adoption?
- Q2.** What behavioural antecedents are most relevant in driving password manager adoption by smartphone users?
- Q3.** Can a recommender system that meets the users' autonomy, relatedness and competence needs encourage smartphone users to adopt a password manager?

The following objectives were set to achieve the research aim:

- 1. Understand the password problem and review the literature that has tried to address this problem; including password managers,
- 2. Explore the current state of password manager adoption,
- 3. Identify strategies to support the adoption of password managers,

4. Find and empirically test smartphone users' significant behavioural antecedents for adopting password managers,
5. Design an intervention to encourage the adoption of password manager applications among smartphone users,
6. Apply self-determination factors in the intervention, and
7. Experimentally test the impact of applying self-determination factors in the intervention on encouraging the subsequent adoption of password managers.

1.3 Research Contribution

The main contributions of this research can be summarised in the following points:

- **Identifying the research gap:**

The literature review is provided to gain a better understanding of the state of the art of the password problem and the research effort that has been made towards solving this problem. It has been found that the proposed solutions and techniques do not solve the password problem. Moreover, there is an apparent lack of human-centric security studies considering the adoption of password management applications.

- **Identifying the adoption stages of password managers:**

A qualitative study was conducted to understand the current state of password manager adoption and the factors that impede or encourage the adoption of a password manager. The data was analysed using Grounded Theory, and it was found that the adoption process of password managers goes through six stages. Accordingly, recommendations were suggested to improve the adoption of password manager applications.

- **A migration theoretic-based analysis of adopting password managers:**

An integrative framework of password manager migration is developed using migration theory as a theoretical foundation. It presents and empirically validates the factors that encourage or deter the intention to adopt a password manager application among smartphone users. The research draws attention to migration theory to demonstrate the migration from password coping behaviours to the use of password manager applications. It introduces migration theory as a referent theory that can be applied to understand other phenomena in information security studies.

- **Designing of an effective information security intervention:**

An intervention to encourage the adoption of a password manager was designed and experimentally validated. It was specifically designed as a recommendation system to support

the adoption stages of a password manager from the user's point of view. It successfully convinced 30% of the participants to install a password manager, which is considered a relatively effective intervention rate.

- **Applying self-determination theory in information security interventions:**

Uniquely, this research has applied SDT in information security interventions. Using a 2*2*2 factorial experiment design method, the research provides evidence that supporting the three basic needs in SDT, in particular autonomy and relatedness, is effective in encouraging the adoption of a password manager. This suggests that applying SDT intervention for information security was appropriate.

- **Identifying the most preferred password manager features:**

The research also contributes to the body of knowledge on password managers by identifying the most preferred features of these applications for the end users. These findings can be used for future research to design a password manager application that satisfies end users' requirements and expectations.

1.4 Overview of the Thesis

The rest of the thesis is organised as follows:

- **Chapter 2** gives an extensive and comprehensive review of the literature related to this thesis. This chapter begins with a brief review of knowledge-based authentication and text-based passwords. Then, section 2.3 describes the current password problem. The following section reviews several studies that have explored password-related behaviours for end users using different research methods. Section 2.5 presents studies that proposed schemes for trying to improve the security of text passwords. Next, section 2.6 discusses other proposed approaches to replace text passwords. The last section reviews password management systems, their main features and types, and the existing studies that consider these applications.
- **Chapter 3** describes an exploratory study that collected data from two sources to understand the current state of password manager adoption and the factors that impeded or encouraged the adoption of a password manager. Grounded Theory was used to analyse the data and the theory of password manager adoption stages, which emerged from the data, is reported.
- **Chapter 4** gives a background of theories and techniques covered in the thesis, including migration theory, SDT, measuring actual information security behaviours and recommendation systems.

- **Chapter 5** presents and empirically validates a theoretical model of smartphone users switching to password managers, using migration theory.
- **Chapter 6** reports on an investigation into the impact of a password manager recommender system that satisfied the three core tenets of SDT: autonomy, relatedness and competence. Then, it discusses users' preferred password manager features.
- **Chapter 7** discusses the findings and reflects on them, providing some implications based on the findings.
- **Chapter 8** summarises the research, discusses its limitations and concludes by suggesting avenues for future research.

Chapter 2

Literature Review

2.1 Introduction

This chapter provides an extensive and comprehensive review of the literature related to this thesis. It begins with a brief review of knowledge-based authentication and text-based passwords. Then, section 2.4 describes the current password problem. The following section reviews several studies that have explored password-related behaviours for end users using different research methods. Section 2.5 discusses different users' password-related behaviours. Then, section 2.6 presents studies that proposed schemes to try to improve the security and usability of text passwords. Next, section 2.7 discusses other proposed approaches to replace text passwords. The last section reviews password management systems, their main features and types, and the existing studies that consider these applications.

2.2 Knowledge-based Authentication

Authentication is a crucial topic in information security. It has been defined as the process of confirming that the identity claimed by the user requesting access to a system actually belongs to them [38]. The existing authentication methods are categorised into three categories based on their characteristics: 1) what the user knows, such as a secret password (also known as knowledge-based authentication); 2) what the user has (e.g. security token); or 3) what the user is (biometric) such as a fingerprint [38].

Authentication is the first line of defence for information systems and it is used to protect resources and services from unauthorised access. However, as the authentication process is a secondary task required to accomplish a primary task, users often do not take enough care over it. They may misuse these security systems if they are not convenient to them, leading to vulnerabilities in protecting the information system. This highlights the importance of not ignoring the end user's role when designing authentication systems. Thus, since the late 90s, a new area

of research has flourished to explore the usability of these systems by combining research on human-computer interactions with studies on computer security. As a result, a number of new conferences and workshops began to focus on this topic, such as the workshop on HCI and Security Systems (CHI'03), the Symposium On Usable Privacy and Security (SOUPS), the International Symposium on Human Aspects of Information Security & Assurance (HAISA), the Workshop on Usable Security (USEC) and the European Workshop on Usable Security (EuroUSEC).

Despite the potential strengths of biometrics and token-based schemes [38], knowledge-based authentication is the most commonly used authentication mechanism. In particular, the text-based password is the most widely applied method due its low adoption cost. This chapter reviews the literature related to the text-based password authentication mechanism. It begins by outlining the potential security and usability problems of this method. Then, some of users' password behaviours are discussed. After that, some of the proposed and developed schemas to address these problems are presented. Finally, an overview of alternative approaches to text-based passwords is provided before moving on to background information and password management tools.

2.3 Text-based Passwords

The use of a password or secret word to authenticate has a long history, before the dawning of the digital age. It was mentioned in the ancient folk tale of Ali Baba when he finds that the secret phrase "Open Sesame!" opens the entrance to a cave, in which forty thieves have hidden their stolen treasures. In computer history, the first password was developed in the 1960s by the Massachusetts Institute of Technology to prevent unauthorised remote login to their UNIX system [22].

A text-based password is a sequence of letters, digits, special characters or words. It is used to confirm the identity of the end user. Typically, during system enrolment, users create their passwords and the system stores the encrypted passwords corresponding to the username in a database. To access their accounts, end users have to claim an identity then prove their knowledge of the shared secret passwords to the system.

2.4 Password Problems

There are some security and usability issues associated with text-based passwords. These issues, referred to as "Password problems" [137], arise from the mismatch between the organisation security expectation and human time and their cognitive capacities. According to SANS, representing the security perspective [37], a secure password should have the following criteria:

- Be at least 12 alphanumeric characters long.
- Contain both upper and lower case letters.
- Contain at least one digit (0-9).
- Contain at least one symbol or special character such as: (! \$% & * ?)
- Not contain substrings that can be found in a dictionary (including foreign languages).
- Not contain substrings that can exist in a language slang, dialect, or jargon.
- Not contain personal information such as birthdates, or names of family members, pets or friends.
- Not contain work-related information such as building names, companies, hardware, or software.
- Not contain word, number or keyboard patterns such as "qwerty" or "123321".

A password that satisfies the aforementioned criteria is difficult to crack and guess. Unfortunately, a hard-to-guess password is also hard to remember; and an easy-to-remember password is likely to be easy to guess and crack. The hard-to-remember passwords produced by rigorously following the guidelines for strong passwords lead users to engage in different insecure coping strategies to ameliorate this memory load.

Human memory receives information through the sensory system, holds it for a brief period of time, processes it, and passes it meaningfully to a short-term memory and then to a long-term memory, from which it can be retrieved later [23]. It is cited that the capacity of short-term memory is 7 ± 2 chunks, based on the results of a famous experiment on short-term memory [24]. A chunk is defined as a unit of information such as a letter, digit, word or meaningful data (e.g. date) [24], and it can remain in the memory for 15-20 seconds [23]. In contrast, long-term memory can store unlimited information over a long period of time. The active part of the long-term memory is known as "working memory" and it has information in a directly accessible state that is shielded against interference from other memory contents through attentional control [25]. The loss of information already stored in the long-term memory is defined in the literature as "forgetting". There are two types of forgetting: unintentional and intentional. The latter is caused by motivation to forget unwanted memories. Unintentional forgetting is also called "incidental forgetting", and it has been expounded in two theories: trace decay theory and interference theory. Trace decay theory suggested that the loss of data in memory over a period of time is due to the passage of time. However, the interference theory describes "forgetting"

as retrieving a memory that is disrupted or interfered with, by similar memory traces [26]. For example, studying similar subjects at the same time can cause forgetting due to interference experience.

Besides password memorability, user convenience is another important issue that can result in insecure password behaviour. Therefore, convenience is another essential criterion of authentication systems, from the user's perspective. Convenient password systems should not be too time consuming, either in enrolment, replacement or authentication [141]. To cope with the conflicting requirements of security and memorability, users often tend to give up the security of their passwords for their convenience. An example of this would be when a user has to change a password and use a combination of alphanumeric and special symbols, which may take time and make the passwords even more difficult to remember. This may lead users to write down the new password or reuse an old one. In trying to understand this phenomenon, some researchers have attributed this behaviour to the "compliance budget" [27][28]. This notion highlights the importance of understanding the cost and benefit of choosing strong passwords from a user's perspective. It indicates that users make a rational decision to adopt security measures when the cost-benefit outcome of adopting these systems or behaviours outweighs the cost-benefit outcome of not adopting them. Therefore, the authors of this approach argue that users have a limited budget for complying with security measures and they suggest that any effort that adds some cost should be offset with some benefit from the user's perspective. Another approach refers to a "digital divide" that exists between information-security managers and end users in terms of their perspective of information-security practices. The lack of interaction between these two groups results in a lack of understanding of each other's needs and points of view [29].

During the last decade, different techniques have been introduced to try to improve the usability and security of authentication systems. These include graphical passwords, biometrics and security tokens. However, text-based passwords remain the most commonly used authentication method for network and computer systems [60,81]. Also, this is a preferable authentication method for online users, rather than other more usable ones [63].

2.5 Users' Password-related Behaviours

Several studies have explored end-user password usage and behaviour using surveys, interviews and diary studies. This section will review some of these studies.

2.5.1 Password usage

In the last decade, an increasing number of online services such as social networks have become widely used and many of the existing services moved to the virtual world, for example e-government, e-banking and e-health care. Consequently, the number of password-protected

accounts that an end user owns has increased and continues to do so. Hence, the need to remember increasing numbers of secure passwords has become normal.

In 2007, Florencio and Herley conducted a large-scale study of password usage and password reuse habits. Using Windows Live Toolbar, they collected data from more than half a million users over a three-month period, and found that the average user had about 25 accounts that required passwords, and was logging into an average of 8 accounts a day. They found that the average user had 6.5 passwords, each of which was shared across 3.9 different websites [36].

Through a two-week diary study in 2011, Hayashi and Hong [35] collected 1,500 password events from 20 participants who recorded their password entries in small diaries. They found that the participants accessed an average of 8.6 accounts per day. Xu et al. (2014) [33] proposed a new approach to prevent victim users from exposing sensitive credentials to a phishing site. In their study, they surveyed 50 web users to understand their login behaviours and found that 64% owned between 10 and 30 online accounts, 24% had more than 30 web accounts; while only 12% reported that they had 10 or fewer online accounts.

Stobert and Biddle [6] conducted interviews with 27 participants to investigate their password behaviours. They found that the subjects reported having a median of 27 accounts ranging from 9 to 51, with the majority having email addresses, school or work accounts, and social networking accounts. The reported median number of unique passwords was 5, with a range from 3 to 20. Loutfi and Josang (2015) [34] conducted a study on IT professionals to investigate the passwords of security experts. They collected data from 1,012 respondents from Norway and more than half of them reported that they owned more than 50 online accounts.

A 2015 survey study of password behaviours across high- and low-literacy web users was conducted by Rinn et al. [31]. Using data collected by interviewing 20 low-literacy participants, they found that the median number of password-protected accounts owned by the participants was eight. The majority had communication-related accounts such as email, social networks and online chatting followed by financial-related accounts such as e-shopping and banking. Only 10% had accounts for e-services such as health care. Similar to previous research, the reported median number of unique passwords was low (4 passwords); ranging between 1 and 9 unique passwords.

Zadorozhnyy (2017) [32] conducted an online study with 76 Russian students, to understand the impact of social networking websites on English language learning among students. The author reported that 48.7% of them indicated that they had 4 to 10 active accounts on social networking sites, although the others reported that they had 1 to 5 accounts on these sites.

Generally, the review of the literature on users' online and password behaviour shows that the frequency with which users access their online accounts has increased and the number of their accounts has also increased. However, the number of unique passwords has remained largely

unchanged.

2.5.2 Creating passwords

One of the password security research themes that has benefitted from research attention is password selection behaviour. The selection criteria are often defined as the selection of the keyboard characters and the length of the password. Users are always required to choose a secure password that the user can remember but which is hard to guess. As it is challenging to meet these requirements, many researchers studied users' password-creation behaviours by analysing their chosen passwords using different methods.

Analysing real passwords:

Some researchers have studied end users' password characteristics by analysing passwords from leaked datasets. Although the ethics of using data exposed by data breaches is heavily debated in the arena of information security [43,44], it undeniably provides a realistic insight into the passwords that people choose.

In 2010, Weir et al [45] analysed passwords from datasets leaked from five websites: RockYou.com, FaithWriters.com, Singles.org, Neopets.com and Phpbb.com, ranging from six thousand passwords to 32 million passwords in the RockYou dataset. They found that the average length of passwords was: 7.88, 7.69, 6.62, 6.68, and 7.27 characters respectively. The highest percentage of passwords including special characters was found in the RockYou dataset at only 3.45%, and only 0.14% of passwords in RockYou were 7+ characters long, containing combinations of uppercase, lowercase, digits and symbols. This was followed by 0.11% in Phpbb then 0.03% in the FaithWriters datasets. The top three special characters found in RockYou were the full stop, underscore and exclamation mark, and more than half of passwords in this dataset contained digits. In 64.28% of them, the digits were appended at the end of the passwords and the digit "1" was the most frequently included digit in the passwords.

Again, in 2012, Bonneau et al. [46] analysed a subset of the RockYou dataset that contained 4-digit passwords and 204,508 iPhone lock screen PINs. They found that the sequence 1234 was the most frequent 4-digit PIN number in both datasets. They also found that passwords representing relatively recent years ranging from 1990 and 2012 were popular, which might represent special or recent events to the users such as a birth, graduation, registration or marriage. Later in 2016, Yu and Liao [47] analysed passwords from the RockYou dataset to investigate whether there were repetitive patterns characterising password choice. They found that users used shorter substrings of the same type to make up longer strings, which were then repeated to make up the final passwords. They suggested that the length requirement of a password policy does not necessarily increase security.

The password habits of Chinese network users have been investigated by analysing 20 million

passwords leaked from four websites: Renren Network, 178.com, 7k7k.com, and CSDN.net: The Chinese Software Developer Network website has accounts of the best programmers in China and hence represents the passwords of Chinese computer professionals [48]. This study found that the average password length ranged from 7.7477 to 9.4571 for the 4 datasets; and the average password length of CSDN users was the longest among the 4 sites, ranging from 8 to 11 characters. They also found that digit-only passwords of network users in China exceeded 50%, while the percentage of passwords including special characters appeared in less than 30%.

In 2016, Shen, et al. [39] analysed over 6 million passwords leaked from CSDN and they measured their characteristics in terms of password length, password composition and password selection. They found that the average length was 9.46 characters and 45% of passwords consisted of only digits compared to only 3.29% passwords containing symbols. They found that the easy-to-reach symbol of the full stop was the top-used symbol in the analysed passwords, followed by the special characters: '@' and '!'. Further to analysing the passwords' characteristics, Shen et al [39] compared their results with the results of eight previous studies from 1989 to 2010 and found that average password length was at least 12% longer than previous results. However, they found a significant increase in using only numbers as passwords and, combo-meaningful passwords. A combo-meaningful password is a password that consists of multiple types of meaningful data (e.g., the combination of a city name and a car name).

Han, Gang, et al (2017) [41] analysed over 141 million passwords collected from datasets leaked from 16 websites. They categorised these datasets into three categories: two email services (Type A), the CSDN.com the Chinese software developers network (Type B), and other websites such as microblogging, forums, gaming, or dating (Type C). They found that the average length of passwords in Type A and Type C was less than the average password length of CSDN passwords (8.08 and 9.43 compared to 8.31). Special characters appeared in only 2.66% of the passwords, and the use of uppercase letters appeared in only 10.48% of passwords, with 8.18% using the letter 'A'.

BoÅanjak and Brumen (2016) [53] analysed textual passwords, used by the students of a Slovenian university to access several online university services (i.e. online grading system, student email, learning material repository, university Wi-Fi network certificate). They found that 20,119 passwords out of 31,184 passwords created by students were less than 8 characters long. About 1.32% of all user-generated passwords included special characters and only two of the generated passwords contained uppercase letters, and none of them contained both uppercase and lowercase letters. Using the same dataset, Taneski et al. (2016) [54] compared passwords generated by students from the tourism school and those created by students from the computer and electric engineering school. They found that students at the faculty of tourism generally created stronger passwords than students at the faculty of electrical engineering and computer science. The latter tended to create passwords that contained single case letters and 3 or more digits, while most of the passwords created by tourism school students consisted of mixed-case

letters and 3 or more digits.

Another approach used to analyse real-life passwords is collecting hashed passwords instead of plain text. Wash et al. [30] used web browser plugins for both Google Chrome and Mozilla Firefox to measure the actual online behaviour of 134 students over the course of six weeks. They found that the average subject used passwords of 8.9 characters length with 2.29 different character types. They also found that only 14% of the passwords included a symbol.

Studying the real passwords showed that the passwords were constructed insecurely. Although password length has slightly increased over time, which might be a result of the strict password requirements, users still use predictable and easy-to-crack passwords. While studying real passwords helps us to understand realistic password behaviours, they do not give us insight into the causes of these behaviours.

Password creation in experiment studies:

An alternative approach to study password interaction behaviour is conducting experiments that mimic the real situation of password creation, where participants are requested to create passwords for fictional websites.

End-user password choices were investigated in an online study using data from 93 participants from a global community of general users [59]. Respondents were not told that the purpose of the study was the analysis of password selection strategies. First, they were required to create an account by filling in their email as the username, and providing a simple password. After submitting their password, regardless of how simple or secure the password was, the participants were prompted to create a more secure password. They were then asked to complete a survey. At the end of the survey, they were asked to recall their initial password, and their revised password. The researcher found that the 'revised' secure passwords that could be recalled later by the participants contained substantial substrings of the initial simple password chosen earlier. Difficult-to-recall passwords were complex and more likely to be substantially different from the simpler ones created earlier.

Hancock et al. (2016) [58] empirically studied the password strength created by end users from the USA and end users outside the USA. Participants were asked to create a secure password that was hard to guess, in order to capture their initial idea of a secure password. This was immediately followed by a prompt to revise their password and input a more complex password (no matter how complex their initial password). They found that there was no significant difference in password selection security or memorability between the passwords that were created by USA participants and Non-USA participants.

Shay et al. (2014) [61] asked 8,143 Amazon's Mechanical Turk (MTurk) participants to create a password, fill out a questionnaire, and recall their password. MTurk is a crowdsourcing website

in which tasks are distributed to a population of anonymous participants for completion. Two days later, they were asked to return and recall their password again and fill out a second questionnaire. The researchers identified the most common substrings within passwords and found that passwords containing five of those substrings were significantly more likely to be cracked than passwords that did not contain them.

Ur et al. (2015) [56] asked 49 participants to create passwords for website accounts while thinking aloud. Then, they interviewed them about their general strategies and inspirations when creating passwords under three different composition policy assigned round-robin bases: 1class6, 2class8 and 3class12. The median password lengths were 10, 9 and 13 characters, respectively. They found that many users used algorithms to create their passwords

Self-reported password-creation behaviour:

A different approach to capturing the password-creation behaviour of end users is to ask them to report on how they choose their passwords. This was achieved by using online surveys in the form of questionnaires, interviewing end users or conducting diary studies.

Grawemeyer and Johnson [60] undertook a diary study of password behaviour involving 22 participants over seven days. Participants were asked about the characteristics of their passwords. They found that users often integrated common words or names into their passwords or used variations of meaningful phrases.

Using interviews, Stobert and Biddle [6] asked participants what they would do when creating an account if their password was rejected because of insufficient complexity. The majority of their participants reported that they would append a symbol. They added that users had a habitual symbol that they used in this situation. The study also revealed that if users knew their password would need a special character, they would have started their passwords with a symbol.

Using a self-report online survey, Farcasin and Chan-tin asked 631 university members about their passwords to understand how they deal with the university's password policy. At password creation, the university provides four randomly generated passwords, as well as an option for the users to create their own passwords under stringent requirements. Only 13% of participants used the pre-generated password and 44% of those who used it considered it a secure password [65].

Shay et al. (2010)[62] conducted a paper-based survey of 470 participants from Carnegie Mellon University who had changed their university password to comply with the new requirements. They collected different data concerning password behaviour; which included password composition. They found that users commonly based their passwords on words, names, or public information such as an address, phone number, or birthday. Also, they found that, of 32 symbols, only 26 were used and the most frequently used symbols were '!' then '@' and '#', which are produced by pressing Shift and the numbers 1, 2, or 3 respectively on a standard international

keyboards (e.g. Mac or Windows) .

However, Taneski et al. [54] found that students' answers to an online questionnaire regarding their password characteristics were not in line with actual university passwords collected in plaintext. They suggested that using a questionnaire as a tool for analysing characteristics of users' passwords might not be delivering realistic answers or trustworthy insights.

Users' perceptions of password security:

Some researchers have studied password choices using online surveys or in lab settings in order to shed light on password-creation behaviour. However, in this approach, participants might be biased towards security when creating their passwords in the lab and may show behaviours that do not align with their actual password behaviour. Thus, this approach might be more suitable for investigations into users' perceptions of password strength than reflecting on their actual password behaviours.

The first study that explicitly studied users' perceptions of password security was conducted in 2016 by Ur et al. [64]. They designed an online study asking 165 participants to rate the comparative security of a set of carefully juxtaposed pairs of passwords, as well as the security and memorability of some password-creation strategies. They found that the participants had some critical misconceptions about password security. They often overestimated the benefit of including digits in passwords and underestimated the predictability of common keyboard patterns and common phrases such as "iloveyou". Interestingly, they found that users' perceptions of what characteristics make a password more secure matched the performance of today's password-cracking tools. They suggested more research to encourage users to apply their perceptions of secure passwords when creating their passwords.

Lo [59] asked participants in an online survey to create a password without any instruction then, no matter how strong or weak their password, the survey prompted for a more "secure" password without any explicit instruction on how the password should be created. This gave them a chance to capture what people really thought in terms of what makes passwords secure. They found that many passwords regarded as more secure contained substrings of the "less secure" passwords, which means that the new "secure passwords" still carried the same security risk as the initial "less secure" passwords. Also they found that users replaced some characters in the initial passwords with others (such as replacing "a" with "@", "o" with "0" or "s" with "5") to create a more secure password.

Shay et al. (2016) [66] used Amazon's Mechanical Turk crowdsourcing service (MTurk) to study users' password behaviour under different password policies. Within their study, they asked participants whether they agreed with the statement, "If my main email provider had the same password requirements as used in this study, my email account would be more secure." Participants who were asked to create a password with at least 8 characters, containing four

classes of characters, were more likely to agree to the statement than in any other condition except the group who used a '16 characters with three classes' password policy. This indicates that users perceived a password that contained differed types of characters to be more secure. Ur et al. (2015) [56] conducted an interview study on password creation using a think-aloud methodology to explore users' perceptions of password security. They asked 49 participants to create passwords for fictitious banking, email, and news website accounts while thinking aloud. They found that some weak passwords resulted from users' misconceptions about secure passwords, such as the belief that adding the special character "!" to the end of a password makes it more secure, or that passwords that contain difficult-to-spell words are more secure than those that have easy-to-spell words. They found that users believed that using personal information such as a birthday or name would be secure if this information was not available publicly e.g. on Facebook.

Knowing the password perceptions of a particular audience is beneficial in order to design effective password policies or password-creation instructions. Further research is needed to understand whether password perceptions differ between low- and high- literacy users, and to investigate the factors that contribute to building password conception, including whether or not these are affected by cultural background. However, even if the users have the correct security perception of what makes a password secure, applying these perception on their actual passwords can not be assured.

Password creation on mobile devices:

With continuous smartphone and tablet innovations, users are relying more often on these mobile devices to interact with the digital world. As these devices have advanced capabilities similar to personal computers, many users rely on them for carrying out an increasing number of activities, which often involve sensitive data. Due to design limitations in these devices such as screen size and soft keyboards, typing secure passwords on these devices is different from typing on traditional keyboards. However, most of the existing research on password behaviour has only focused on their use on personal computers. Little research highlights the effect of smartphone device platforms when creating and using passwords.

Melicher et al. [57] studied passwords created on smartphone devices and found that creating passwords on mobile devices takes more time and results in more errors and greater user frustration compared to creating passwords on desktops and laptops. They found that mobile participants included fewer symbols and uppercase letters in their passwords than hard-keyboard users. They showed that mobile passwords are less secure than traditional passwords against offline guessing attacks.

Von Zezschwitz et al. [3] studied the influence of mobile devices on authentication performance

and password composition. They conducted a lab experiment followed by a large-scale survey comparing the impact of device type on password creation using three device classes: desktop, tablet and smartphone. They showed that passwords of the same complexity performed significantly slower on mobile devices and thus users tended to use passwords that were easy and fast to enter on smartphones and tablets. Therefore, user-defined passwords were significantly shorter on smartphones than the ones created for desktops. They also found that mobile devices were commonly used when choosing new passwords, as reported by participants, which might negatively affect the overall password security.

The impact of smartphone use on password authentication and password selection is still a rich area for further research (e.g. understanding the effect of password strength meters or other password policies on constructing passwords using smartphones). Furthermore, giving that smartphones were commonly used when creating new passwords[3] and due to the fact that users often choose a simple password when using soft keyboards ,for faster typing and login time [3] [57] , there is a need to support smartphone users to create and use more secure passwords for their online accounts.

2.5.3 Changing passwords

Because of the regular data leaks happening from large and small companies and websites, it is recommended to change passwords in order to protect users' accounts from this threat. Therefore, some researchers investigated changing password behaviour.

Using a diary study of 22 participants over 7 days, Grawemeyer and Johnson (2011) [60] investigated how often participants changed their passwords. They found that the majority of passwords that participants reported for the different services were never changed (139 out of 175); 17 were changed more than once per year; 16 were changed up to once per year; and 3 had been changed once.

Stobert and Biddle (2015) [91] found that changing passwords was a stressful task for most users. They found that most experts said they seldom changed their passwords and mentioned some of the challenges of this practice. However, they were more likely to report that they changed their passwords than non-expert participants. They also reported that a number of their participants mentioned having had their password since they had started using computers and one revealed having had her/his password since high school.

Fredericks et al. (2016) [69] compared students' password knowledge and their reported behaviour at a university in South Africa. They found that most students reported that they believed they should change their passwords every 90 days but only 13% of these students indicated that they changed their passwords every 90 and 16% of them reported that they never changed their passwords.

Using a total of 185,643 plaintext passwords, Bosnjak and Brumen (2016) [53] showed that the vast majority of students in a slovenian university continue to use the generated default passwords for their university accounts and the large majority of the rest of the students who had changed their passwords created short passwords that mainly consisted of alphabetic or numeric characters.

Although it may improve the security level of passwords, changing passwords adds an extra burden to the password usability problem. Therefore, many end users may avoid this practice and do not change their passwords unless they have no choice. That is when they are forced to change them due to a password expiration policy or when they forgot their password. However, users may create weak passwords or practice insecure password behaviour when they are enforced to change their passwords. Because enforced changes make passwords weaker, NIST new guidance [139] recommends never forcing a password change unless there is evidence of a breach.

2.5.4 Reusing passwords

One of the strategies used by end users to cope with remembering multiple passwords with restrictive password policies is to reuse passwords across multiple accounts or recycle them by slightly modifying the passwords. This practice has a security risk due to the potential domino effect that can result if one site's password dataset becomes available to a hacker who then uses it to penetrate accounts in other systems and to access more accounts [70]. Despite this security risk, the vast majority of end users still reuse their passwords. Therefore, many studies of password behaviour have considered the password reuse practice.

In 2006, Florencio et al. [36] found in a large-scale study, conducted with half a million users by monitoring their passwords over 3 months, that on average each password was reused across 3.9 accounts and a very large number of weak passwords were reused more than strong passwords. However, ten years later, Wash et al. [30] found that strong passwords were more frequently reused. This might be due to password policies now being stricter than ten years ago. Grawemeyer et al. (2011) [60] showed, in a diary study for a week, that half of their participants reused their passwords across four authentication systems. Shay et al. (2010) [62] found in a survey that more than 50% of participants reported that they either modified an old password or reused it. Similarly, Choong et al. (2015) [68] found that 56.6% of 4,573 employees in an USA organisation reported that they reused their passwords for at least half of their accounts. An interview study that investigated expert password behaviour [91] found that most of the experts reported that they reused passwords on at least some of their "throwaway" accounts with a median of 3.5 reused passwords. In a lab experiment, Ur et al. [56] investigated the password behaviours of 49 users, creating accounts at three fictitious web accounts. They found that only 3 users created

a unique password for each of the three accounts, and 18 of them recycled the same password by adding extra characters or words or slightly modified it, such as using "ATdim12nd#, ATdim12sw#, and ATdim12ft#", where the last two letters represented the names of the sites. They concluded that while some users were aware that password reuse is a risky practice they did so anyway, and others still failed to see this behaviour as potentially problematic for their accounts. However, because the experiment was conducted in the lab, this result may not be ecologically valid.

Despite the risk of reusing passwords across many accounts, end-users continue to practice this behaviour. This highlights the need to support users to avoid reusing passwords without burdening their memory.

2.5.5 Recording passwords

Writing down passwords is another common technique that end users adopt in dealing with the password problem. This strategy gives users an opportunity to create a secure and unique password for each of their accounts without suffering from issues remembering them. However, this behaviour creates a serious security threat for users' accounts if the recorded passwords are exposed by attackers.

Stobert and Biddle [91] found that more than half of their participants reported that they wrote some passwords down as a kind of backup strategy. Choong and Theofanos (2015) [68] found that those people who perceived password strength requirements as burdensome were more likely to write them down on paper and store them in files; Also, they were less likely to trust their memory. Furthermore, they reported that they wrote their passwords in plaintext more often than users who thought the password requirements were about right.

Petrie and Merdenyan [73] found that many users reported that they recorded their passwords and that they did not believe that writing passwords down significantly compromised their security. They also found the most commonly mentioned systems, where participants wrote down their passwords, were online banking and email services.

This strategy is not a bad practice in itself and it may help to improve password security but only if the passwords themselves are securely recorded in a file that is stored in a safe place [72]. However, it has been found that writing down passwords did not significantly improve password security or memorability [71]. Further, Shay et al. (2014) [62] found that about 30% of participants who reported that they recorded their passwords did not protect their password records at all.

2.5.6 Sharing passwords

Although passwords are assumed to be personal and confidential, password sharing is common among end users. It has been found that the majority of shared passwords were shared with family members [73].

Singh et al. pointed out three reasons for password-sharing behaviour:

- (1) sharing passwords as a demonstration of trust, especially among couples and family members;
- (2) sharing passwords for necessity in some daily life incidents (such as when one asks someone else to access her/his account while driving a car) and
- (3) and sharing passwords to provide assistance to other users such as people with special needs who depend on carers [76].

A study found that two-thirds of couples in committed relationships had shared passwords. Some of them shared email addresses and social media profiles as a couple [75]. In a survey, Kaye studied how passwords were usually shared between friends, partners and family members. The result of his study shows that one-third of users reported that they shared their personal email password, compared to one-quarter who shared their Facebook passwords, both mainly with partners and close friends [78].

Not only adults, but also young users share their passwords. A report in 2012 shows that teenagers were giving each other passwords to their social networking accounts as a sign of trust and devotion [79]. This may even be worse because of the potential risk for involvement with cyber-bullying among young users who regularly use social networking accounts [77].

Whitty et al. (2015) [74] found in a survey that younger users were more likely to share passwords compared with older people and that participants who scored high on lack of perseverance were more likely to share their passwords. This means that people who tend to delegate an on-line task to others to complete, in order to minimise boredom and personal effort on the task, are more likely to share their passwords than others. Also, they found that those who scored high on self-monitoring were more likely to share passwords than those who scored low; which suggest that users who observe and regulate their expressive behaviors are more likely to feel pressured by others to share their passwords. Petrie and Merdenyan [73] showed that culture and demographic background might affect users' decisions to share their passwords. They found in a self-reported study that women were more likely to share their passwords than men did. However, participants from Turkey reported that they shared their passwords more than participants from China and the UK.

Sharing passwords can be essential for some users, as it establishes trust and convenience. However, this behaviour may be harmful to security if these passwords are reused to access multiple accounts.

2.5.7 Summary

Despite knowing the impact of poor password behaviours by end users, managing unique passwords for many accounts securely is challenging and too much of a burden. Therefore, people continue creating weak passwords, reusing them, writing them down and sharing them insecurely, and password insecurity persists.

2.6 Schemes to improve Text-based Passwords

In trying to improve the security of text passwords, many schemes have been proposed and/or applied. Some service providers prevent weak passwords by offering the users system-generated passwords, while others enforce strict password requirements. Some approaches offer real-time password-creation feedback that dynamically shows whether users have met the requirements or feedback that shows how strong the created password is, such as using a password strength meter. Other service providers offer guidance: explaining how to create a good password. Some researchers have proposed novel techniques to improve text passwords by adjusting the user-created passwords. This section will review some of the studies that have attempted to improve text passwords.

2.6.1 System-generated passwords

To avoid the weaknesses of end-user chosen passwords and instead of teaching them how to create a secure password, authentication systems may assign a system-generated password. System-generated passwords are stronger than user-generated passwords. Yet, users tend to remember their own passwords better than those assigned to them. [96]. Ranganayakulu [96] compared the usability of a novel system-generated mnemonic password policy with three existing password policies, while maintaining a constant level of security across the four policies. He found that the user-generated password policies (user-generated password policy and user-generated mnemonic policy) were more usable than the system-generated policies (system-generated password policy and system-generated mnemonic policy). Farcasin and ChanãŔtin [65] performed two surveys to understand the password behaviour of university members. In particular, they studied users' perspectives regarding the university password policy, which offered users four pre-generated random passwords, with the option to create their own password, subject to stringent requirements. They found that most people chose to create their own passwords and used coping strategies to deal with the requirements and thereby subvert the security of the passwords. They concluded that a pre-generated random password is an unusable security strategy for most people.

Because system-generated passwords are typically meaningless, they are hard to remember.

Therefore, Shay et al. [97] explored the usability of 3- and 4-word system-assigned passphrases in comparison to system-assigned passwords. They found that system-assigned passphrases performed similarly to system-assigned passwords of similar entropy across different usability metrics. Both passphrases and passwords were forgotten at similar rates, had similar levels of user difficulty and annoyance, and both were written down by a majority of users. In addition, more passphrases took significantly longer for users to enter. Nevertheless, pronounceable random passwords were easier to remember and enter. Wright et al. [98] found no improvement in memorability between recalling system-assigned passwords and recognising passphrases by selecting the assigned words from lists of displayed words. They also found that recognising the assigned passphrase took longer to authenticate successfully.

In summary, system-generated passwords can improve the security of passwords; and yet these passwords are not preferred by end users as it is cumbersome to memorise them all.

2.6.2 Enhancing user-generated passwords

Another approach to enhance text passwords is to improve a user-created password in order to strengthen it. Some researchers have proposed techniques to improve password strength by replacing or adding some random characters to a user's password [92,93]. Generally, they found that their proposed technique could increase the security of user passwords. However, the usability did not improve [92,93]. Segreti et al. [95] tested the effect of applying an adaptive password policy that asked the users to adjust their passwords if they detected common passwords, and suggested inserting a few characters to strengthen the passwords. They found that the created passwords were more resilient against guessing attacks with no effect on creation or recall time. This approach addresses the security problems of passwords by helping end users to create secure passwords. However, password memorability remains an issue.

2.6.3 Password instructions at creation time

Another approach to improve text passwords is educating end users about how to create a good password. Users often do not understand the password policies and the rationale behind them. Some system administrators provide instructions and advice while users create their passwords. Guiding users to create passwords improves the security of the created password in terms of length and complexity [20]. However, the password-creation instructions are not always understood by end users.

Furnell [20] examined the password practices of ten popular websites. They found that the majority of sites provided little or no guidance on how to create a good password. Their password restriction policies and password guidance were very different, and conflicted with one

another. Further, they found that password instructions were often ambiguous and unhelpful; which might make it hard for the users to know how to create good passwords.

[40] investigated user understanding of ambiguous terminology in password rules. They found that there is ambiguity in the language used to indicate special characters. In particular, users were confused by the terms "non-alphanumeric", "symbols", "special characters" and "punctuation marks" in password rules. Furthermore, they found that users often took password rule language literally. For example, they interpreted the language "[...] must contain one special character" in the password instruction as meaning literally that "only one" special character was allowed. Technical terms like "non-alphanumeric" were found to be confusing to users and spaces were not recognised as characters. Also, users were confused by partial lists of allowed characters using "e.g." or "etc."

Althubaiti and Petrie [142] investigated different types of instructions that are provided by password-creation systems. They found that only 10% of the instructions were provided before the interaction with the authentication system. They also conducted an online study to investigate users' perceptions about the password instructions. They found that users prefer to see the declarative policy before interacting with the system. Declarative information provides exploratory information, such as the statement: "A good password is hard to guess". Moreover, they found that users prefer declarative creation suggestions to other types of suggestions before, during and after interaction with the password-creation system, for example: "You can improve your password by adding jokes".

2.6.4 Mnemonic strategy

In order to create a strong but still easily memorable password, it is often recommended to memorise a random mnemonic sentence and concatenate the words' initials to construct a so-called 'mnemonic password'. This strategy was originally proposed by Barton and Barton in 1984 [99] on the basis that passwords that appear to be meaningful to the user are easier to remember.

Yang et al. [100] investigated the security of 6 different variations of the "create a sentence" part of the mnemonic password strategy. They found that a well-designed explicit instruction for choosing a personalised mnemonic sentence that is unlikely to be chosen by others, with an example of a password generated using a mnemonic sentence, can increase the security level of the resulting passwords. They also examined the mental workload and memorability of 2 mnemonic strategies and found that the perceived workloads for the mnemonic strategies were higher than when no strategy was required. Unfortunately, evaluating the memorability after 1 week revealed no significant reduction in password recall between the two cases.

Topkara et al. [101] proposed a mnemonic scheme for text passwords that split a password into two parts: a part that is encoded in a mnemonic sentence and another part that is written down on paper. This scheme allows the users to maintain a diversity of unique passwords, which can

be recalled by remembering only one mnemonic sentence.

Recently, Kiesel et al. [102] analysed the strength of passwords generated using mnemonic password advice on a large corpus of 3 billion human-written sentences. They analysed password security under 18 different password-generation rules. They found similarity between human-chosen mnemonics and web sentences. Among the 18 tested password generation rules, the strongest password distribution, against an offline attack, was generated by using the ASCII character set by concatenating the first character of every second word and using common word prefix replacements to add more special characters to the passwords. The complexity of the sentence generated using mnemonics has a major effect against online attack when the attacker can try a only few guesses (usually 3 times). Sentence complexity was measured in the study using standard Flesch reading ease formula that considers the number of words and syllables. Furthermore, they found that the strength of mnemonic passwords against online attacks was not affected by the password length.

2.6.5 Password cue

Another technique that may support text password memorability is cueing.

Camp et al. [103] suggested a system that offers entropy to the user by providing randomly selected images in a password-creation session and utilising them as a visual cue to simplify contextualisation where the user has to map each password to a different account. The evaluation of the proposed system showed a significant increase in entropy and length of passwords created with no decrease in the recall of these more entropic passwords. However, this system may be vulnerable to adversary attack.

Another novel scheme that applied cues to assist password memorability was proposed by Renaud et al. [104]. They developed the Cueblot assisted authentication system, which displays an inkblot-like image to trigger the user's memory when interacting with the authentication system. The system instructs users to use the abstract image to elicit a textual description that could be used as password. The researchers conducted an online study to evaluate the Cueblots and found that the system had a negative impact on usability. Also, the system did not enhance the strength of the chosen passwords. They concluded that users simply do not need cues in authentication systems; rather they only want the password hurdle to be minimised.

Al-Ameen et al. [105] applied the cue technique with system-generated text passwords to address the usability-security tension of randomly generated passwords. This novel cued-recognition authentication technique provides users with different cues (visual, verbal, and spatial) and allows them to choose their preferred cues for future recognition of a system-assigned password. In a lab experiment they evaluated this scheme and found that all of the 37 participants successfully recalled their passwords within three attempts one week after registration. Despite the high memorability of this technique, the study found the login time to be relatively high. Also, the

system was only tested on one password in the short term (one week). The memorability of the text password might not be improved in the long term with multiple passwords.

The cueing mechanism has some drawbacks that make it impractical to apply. Since the cue is available to all users and to attackers, this system is vulnerable to attack. Also, using the system is too time consuming during the authentication process.

2.6.6 Password-creation feedback

Another approach to enhance textual passwords is to provide users with feedback that displays the password strength as it is entered. This typically is provided in the form of a meter that shows how strong the password is. Some feedback strategies are provided by checking a list of requirements that must be included in the created password.

Password strength meter:

A password strength meter is a tool that evaluates the strength of a chosen password when a user creates it, and it displays assessment feedback, typically with different colours indicating the security level.

Khern-am-nuai et al. [82] conducted a randomised experiment on the Amazon Mechanical Turk to test the effect of adding contextual information to enhance the effectiveness of password strength meters, by observing the changes in users' behaviour. They found that providing additional contextual information, along with warning messages displayed by password strength meters, had a positive impact on enhancing the understanding of password strength among users; improving password-generating behaviours. Indeed, participants exposed to the password strength meter with contextual information were more likely to change their passwords after seeing the warning message, and their new passwords were stronger.

In an online user study of over 2,000 participants, Ur et al. [80] experimented with 14 password strength meter alternatives and found that the presence of any strength meter nudges participants towards creating more complex and longer passwords. However, they found that participants who used stringent meters (i.e. meters that scored passwords stringently) spent longer time creating their passwords and were more likely to find the password meter annoying; which may deter them from improving their passwords and cause them to ignore the meter's advice in the future.

In a field experiment setting, a password strength meter was shown to be effective in encouraging participants to create stronger passwords when it was combined with a fear appeal message [81]. Egelman et al. [83] found that meters positively affect the strength of passwords when users are forced to change existing passwords, yet this effect is context dependent.

Although the meter can improve password security, it has no effect on improving memorability

issues. Also, it did not have an observable effect on discouraging the reuse of weak passwords.

Real-time requirements-compliance feedback:

To make the process of creating strong passwords easier, some authentication systems provide real-time feedback, in the form of a checklist, during the password-creation session. Real-time feedback validates the user's input dynamically, which leads to a reduction in the number of unsuccessful password entries or submissions [107]. This typically indicates which of the password requirements are met by providing a checklist that is dynamically checked while the users create their passwords.

Shay et al. [108] conducted a large-scale online study, on the Amazon's MTurk service, examining the impact of real-time requirements-compliance feedback during password creation on the password's security and usability. They found that requirements feedback made password creation less error prone and increased the participants' perceptions of strength. However, real-time feedback had no effect on password strength. Participants were less likely to add extra character classes. This may be due to the effect of real-time feedback on the participants' feeling that they had included what they were expected to include in the password to make it secure. Without real-time feedback, users may not be aware of when the requirements have been met and thus add extra character classes to be sure. The authors suggested that real-time feedback could be a useful feature to improve the usability of the user-interface of authentication systems. Ur et al. [56] (2015) argued that data-driven feedback during password creation could lead to misconceptions and build a wrong mental model about how to create secure passwords (e.g. adding the character '!' to strengthen passwords), which might, actually, make the password more predictable.

Emoji feedback:

Recently, Furnell and Esmael [42] proposed a new technique that utilised Emoji faces to provide feedback and encourage users to create a strong password. They found that Emoji feedback led users to create stronger passwords compared to meters and standard guidance. Despite the positive effect on security, this technique does not improve the memorability.

Informative feedback:

Instead of only evaluating the strength of user passwords and showing whether their passwords are strong or weak, some scholars have suggested that providing users with an exhaustive explanation of why their passwords are considered strong or weak may lead to better password-creation behaviour.

Furnell et al. (2018) [111] examined variations in the form of password feedback messages pro-

vided with a meter-based rating. They found that providing richer information explaining the password evaluation, such as the time required to crack a password, its relative ranking against other choices, or the probability of it being cracked, made users more motivated to change their initial weak passwords to stronger ones.

Komanduri et al. (2014) [109] used training data from a leaked password database and natural language corpora to build a dynamic feedback system, named Telepathwords. This shows users, while they are creating their passwords, predictions about what they will type next. This system showed the users the possible predicted passwords, the point being that if the system could guess the password, attackers may also find the password easy to guess. They found that the technique effectively encouraged participants to create stronger (less predictable) passwords.

Ciampa [112] examined four different types of password feedback mechanisms to investigate the most effective one: a traditional password meter, a dial meter, a detailed horizontal bar that showed the relative strength and an informative message that indicated the length of time necessary to crack the password. They asked participants whether the feedback encouraged them to change their original password when they created their passwords for the four authentication systems. The password feedback mechanism that was most effective was the feedback that showed the estimated amount of time needed to break the password.

2.6.7 Password policy

Password policies are a set of rules that are required when creating a password for a given system, aiming to influence the users to create strong passwords. They are implemented, by system administrators, on most online websites. Password policies can be a list of password composition requirements that must be included in the created passwords, such as a minimum number of characters, the password expiration period and/or blacklisted passwords that cannot be used in the password.

For many years, system administrators used to adopt a standard password policy released by The Federal Information Processing Standards (FIPS)[138] until the National Institute of Standards and Technology (NIST) [139] issued their first password restriction policy in 2006. Since the time when Sasse et al. [113] published their study in 2001, many researchers have conducted studies to compare different password policies in terms of usability and security.

A study conducted by Bosnjak and Brumen (2016) [53] concluded that when no password policies are required, users create weak passwords: short, simple and mainly consisting of alphabetic or numeric characters. Farcasin et al. [65] surveyed members of a university about their perceptions and behaviour regarding the university password policy and found that requiring users to change passwords every 120 days was not usable and led them to apply coping strategies that undermined the security of the password policy.

Habib et al. [114] investigated how users changed their passwords when they responded to a

blacklisted password attempt. They found that participants ,who reused a modified version of a blacklisted password, created significantly weaker passwords. Komanduri et al. (2011) [115] conducted a large-scale user study using Amazon's Mechanical Turk to investigate the effectiveness of several basic password composition policies. These policies varied in length (e.g. basic8 and basic16), blacklist (such as dictionary8) and the minimum number of required character classes (e.g. comprehensive8). Password must have at least 8 characters in password policy Basic8, and it must have at least 16 characters in basic16. For dictionary8, Password must have at least 8 characters and it may not contain a dictionary word. In comprehensive8 policy, password must have at least 8 characters including an uppercase and lowercase letter, a symbol, and a digit; also, it may not contain a dictionary word. They found that users often used predictable strategies to deal with the restriction (e.g., capitalising the first letter of a password if the password policy required including a capital letter). Also, they found in a short-term password recall study that these policies led 31% of participants to write down their passwords. They compared the usability and security of the different policies and found no difference in entropy between basic8 and dictionary8; yet dictionary8 was less usable during creation due to the heuristic cracking that adds frustration to the users. Because of the minimum length requirement, basic16 resulted in higher entropy than comprehensive8 and it was easier to create and recall and less likely to be recorded. Therefore, they concluded that using basic16 provides more secure passwords at a small usability cost. In contrast, comprehensive8 was the least usable policy. Surprisingly, they found that participants often created passwords that exceeded the minimum requirements, thus increasing password entropy. However, the increase in entropy was correlated with a decrease in usability.

Likewise, Shay et al. (2016)[66] examined 15 password policies to test their usability and security focusing on length requirement by conducting two online studies with over 20,000 participants. They found that a length-only password requirement is usable but leads to unsecure passwords. They also showed that 2class12 and 2words16 password polices were more secure and usable than the commonly used comp8 password policy. Their study reveals that including a blacklist in the password policy made the created passwords more difficult to guess without affecting the recall; yet, the password creation was difficult. Therefore, they suggested that this requirement is only suitable for some services that do not seek as many users as possible to create accounts in their services. Similarly, the pattern requirement that requires passwords to start and end with lowercase letters led to less predictable passwords; yet it made password creation and recalling more difficult. They suggested applying this requirement only to high-security service providers. Their study concluded that password strength and usability are not always inversely correlated.

Mogire et al (2017) [94] tested the effect of applying an augmented password by adding bold, italics, underline or strikethrough to the password composition. They found in a usability study that the recall rate was better (over 90% recall) for the augmented passwords compared to the

non-augmented passwords. Further, increasing the password entropy enhances the security of these passwords.

A study from Segreti et al. (2017) [95] investigated the usability and security of adaptive password-creation policies, which dynamically changed the requirements over time as users created new passwords. They found that a well-designed structure-based adaptive password policy significantly increased the security level of the created passwords with little to no decrease in usability. This policy prohibits users from creating passwords with the same character class structure (pattern of symbols, digits, and letters) as another user's password; each time a new password is created, its structure is considered as "in use" and is not allowed during future password creation attempts.

2.6.8 Password chunking

Because people, generally, remember information using the chunking technique, by grouping several smaller chunks of information into a fewer larger ones, Bishop [118] has suggested that passwords should be composed of chunks (i.e. groups of characters, numbers or both) that are only meaningful to the password's creator.

Huh et al. (2015) [119] investigated the impact of chunking techniques to improve memorability for larger PIN lengths. Their study shows that chunking generally improves memorability of system-generated PINs. Interestingly, however, none of the individual chunking policies (e.g., 0000-00-00 and 00-0000) significantly improved the usability compared to their corresponding non-chunked policies (e.g., 00000000 and 000000).

Carstens and Malone [120] evaluated the impact of password guidelines for authentication based on chunking theory. Their study findings show the advantages of applying two-chunks to four-chunks of data to increase password security while reducing the demand on the user. They found that passwords that are composed of meaningful data for the password creator, and which meet minimal security requirements, were easier to recall and less prone to poor password practices that compromise overall security.

Although the evaluation of these schemes shows an improvement in the password strength, their impact may not be practical if we apply them to various accounts. In particular, it may be cumbersome to map each chunk of data to a particular password and to map each password or group of chunks to a particular account. Hence, the usability and security problem of text passwords still persists.

2.7 Other Approaches to the Password Problem

2.7.1 Single-sign-on

Single sign-on (SSO) provides a single authentication entity that allows a user to access multiple accounts with one set of login credentials. The typical SSO architecture involves the SSO provider, the relying services and the end user. There are different implementation examples of SSO, such as OpenID, OAuth, or utilising commonly used social networking accounts as SSO providers (for example, Facebook, Twitter and Google).

Scott et al. (2016) [121] conducted a survey to examine the usage and perception of individuals regarding SSO schemes and found that the majority of the respondents prefer registering on a website using an entirely new account, rather than using a "Sign in with Facebook" option.

Sun et al. [122] empirically investigated OpenID to understand why SSO was refused by end users and found that many participants incorrectly thought that the OpenID credentials were given to the content providers. They also found that users did not perceive the usefulness of SSO and many had concerns about using this technique on accounts that contained valuable personal information, or on websites that were not trustworthy.

Despite the improvement in usability, this technology is not widely adopted by users [121] and [122]. Also, this approach does not offer any advantages to the security of the passwords. Moreover, it needs to be deployed by system administrators. Further, users have to have accounts with the SSO providers; which might not be necessarily the same SSO provider for each service. In addition, if one SSO provider goes down, access to all related web accounts is lost, and if it is hacked or breached, data loss may occur.

2.7.2 Token-based authentication

Token-based authentication (TBA) was proposed to allow users to authenticate using physical or electrical tokens held by the users to claim their identity. The token can be either static information such as a cryptographic key or a dynamically generated token such as a One-Time Password (OTP); based on a time or counter. A token is classified as hardware or software: hardware are physical portable devices such as a smartcard or Yubikey, while software tokens are programs that can be embedded into existing smart devices to get the secret token, such as SMS messages or OTP authenticator applications. The latter is more convenient and less expensive to apply.

The authentication process using the token technique can be connected, contactless or by manually entering tokens. To apply a connected token in an authentication system, a special reader device is needed to read the token's information (such as a USB port and smartcard reader). To use a connected token, end users have to plug it in at the authentication time, and the token

information will be transmitted automatically to the authentication system. Contactless tokens need wireless connection technology such as near-field communication (NFC) to send the token information to the authentication system. The manual tokens do not require a physical connection to send the token information; instead, users are required to enter it manually into the authentication system.

Krol et al. [123] studied the impact of using authentication tokens in UK online banking on user experience. Over a period of 11 days, they collected a total of 90 login sessions from 21 bank customers and the analysis showed that 13.3% had usability problems such as mistyping authentication credentials or misplacing the token device. They found that using a hardware token was inconvenient and a source of frustration to the users; which led to a decrease in the frequency of logins to their bank accounts. Furthermore, users reported less satisfaction with the online banking login experience when they had to use a hardware token with more login steps. Recently, Das et al. [124] examined the usability of the Yubico security key by implementing a think-aloud protocol, documenting the halt and confusion points to generate many recommendations for Yubikey. After Yubico implemented the recommended changes they, repeated the study and found significant improvements in the usability. However, the improvement in usability did not affect the acceptability of the device due to perceived un-usefulness and risk concerns over losing access to accounts.

This approach avoids the problem of password guessing attack. However, these token devices can be lost or stolen and then used by an adversary user to access users' accounts. Therefore, this scheme is often used with another authentication factor, typically text passwords. Nevertheless, if the token is lost, the legitimate users will not be able to access their accounts. Entering an authentication token manually is inconvenient and time consuming, whereas transmitting the token information automatically needs a special device such as a smartcard or Yubikey, which is expensive to apply, especially in large organisations. Also, it is a burden to carry authentication devices; even worse if users have to manage several tokens for different accounts.

2.7.3 Biometric authentication

Biometrics relies on the measurement of users' unique physiological or behavioural characteristics for authentication. Examples of physiological characteristics are: fingerprint, iris scan, and voice recognition, whereas keystrokes and signature scans are examples of behavioural characteristics. Since biometric authentication does not require cognitive effort or carrying a special device, it improves the user experience. Besides being a usable authentication solution, it improves the security. Nevertheless, this technology has some limitations that affect its widespread adoption. Al-Daraiseh et al. [125] found in an online study that although 76% of iPhone's users believe that fingerprint technology enhances the security of their devices, only 33% of them

reported that they applied it to lock/unlock their devices and only 16% of them said they used the fingerprint to buy from iTunes. Interestingly, only 31% of the study participants reported that they had concerns about using the fingerprint feature, and these were mainly related to privacy breaches. Alongside the privacy concern, they reported a risk-concern of losing or abusing this personally identifiable information in the case of compromising the database, which cannot be reset once compromised. Another drawback of applying this technology is the cost of integrating it into authentication systems and the cost of using and maintaining additional hardware such as the fingerprint scanner. Furthermore, these systems are not 100% accurate and cannot be applicable to all users. Users with some defects in biometrics, such as an injury to their thumb, cannot be authenticated using the biometric authentication system [126]. Also, the widespread use of facial plastic surgery and the use of Botox or fillers to change face shapes and characteristics is another factor that negatively affects the accuracy of face detection [127].

2.7.4 Two-factor authentication

In an attempt to enhance authentication security, a combination of two or more authentication factors is used. This is commonly applied using only two factors and referred to as two-factor authentication (2FA). To grant access, users should be authenticated successfully by all the authentication factors. A typical example of 2FA is mixing Token-Based Authentication TBA (such as Google Authenticator or Microsoft Authenticator) with a text password. This technique can prevent guessing attacks, as the attacker has to have the token. In contrast, if an adversary has the token, he/she has to successfully guess the password, thereby decreasing the opportunity of successful account hacking.

Two-factor authentication has been applied by many web services such as Twitter, Gmail and most online banking services. However, this approach does not enjoy acceptance by end users. Petsas et al. [128] examined over 100,000 Google accounts and concluded that 2FA had only been enabled by 6.4% of the analysed accounts. Krol et al. [123] stated that due to the mental and physical workload involved in using 2FA and the number of steps required, many online banking customers dislike them.

2.7.5 Graphical password

In the last decade, on the basis of 'A picture is worth a thousand words', research about graphical passwords flourished and it reached its peak in 2013. A graphical password is a password containing a visual element, which can be a set of images or a sequence of x and y coordinates, aiming to reduce the memory burden of text passwords.

Several applications of this approach have been proposed and tested. They fall into three categories: recall-based systems, cued-recall systems, and recognition-based systems.

Jermyn et al. [129] proposed a recall-based graphical password Draw-A-Secret (DAS) mechanism in 1999. It allows users to freely draw on a 2-D grid as a password at the registration stage and the coordinate pairs of the drawn password are stored in the database. Users are required to recall their drawing in order to log in to their accounts. Dunphy and Yan [130] proposed Background-DAS (BDAS), as an improved version of the original DAS, by adding a background image to improve memorability and to encourage unpredictable passwords. Jebriel and Poet [131] found that it is highly possible to guess others' passwords if they contain cultural characteristics. The DAS approach was applied in Android mobile devices as a screen-unlock scheme. However, Aviv et al. [132] demonstrated the vulnerability of DAS applied on smartphones to "smudge attacks" where an adversary user can determine the legitimate user's password through the finger smudges left on the phone's touch screen.

For recognition-based systems, users are presented with a set of images and they need to recognise the images that they selected previously during registration. The images used in this approach include faces [133], everyday objects, Mikons, Doodles [135], or the users' own photographs [55]. Researchers have proposed many recognition-based systems but Passfaces [133] is the only recognition-based graphical password scheme that has been commercially deployed. In Passfaces, users create their passwords by selecting human faces at registration. Users must then identify their preselected images from amongst distractions each time they need to log in to their accounts. Stobert and Biddle [134] show that a recognition-based graphical password is more memorable than a recall-based one. However, if graphical passwords are widely adopted, a study [135] provides evidence that multiple recognition graphical passwords are difficult to remember, and time consuming to enter.

Cued-recall-based passwords support the user's memory with images when recalling their passwords. An example of this scheme of graphical password is the PassPoints system. The PassPoints system [137] uses images chosen by the user and asks the user to select some points on the selected image as their passwords. At login, the user needs to click on the points that were previously selected on the image. A key security drawback of this approach is its predictability, as users tend to select similar locations on images, forming what are called image hot spots. Also, the sequences of clicks usually form predictable geometric patterns [136]. To overcome these problems and make the selected passwords more secure, Karia, and Patankar [110] used the Fogg principle [117] to design a persuasive click-based technology. Fogg principle has created a universal method for behavior change by specifying the target behavior, making it easy and triggering the users to perform this behaviour. The designed persuasive click-based technique influenced users to select more random and difficult-to-guess points, without imposing system-generated passwords. This technique shades out the entire image except for a randomly

chosen part of the image named ‘viewport’, where the user can choose their clicks.

Although graphical authentication uses the memorability advantage of images to improve password usability, the time required to sign in and log in using these schemes is long. Also, the authentication system requires much more storage space for the images than a textual passwords database. Furthermore, a graphical authentication system is vulnerable to some types of attack such as shoulder surfing and recording attacks [140]. Therefore, very few graphical password schemes have been adopted in practical.

2.8 Password Management Systems

Different solutions have been proposed and/or developed to address password problems. These solutions can be categorised into three main categories. The first category of the solutions aimed to improve how text-based passwords are created uses password policies. However, the password problem is still not solved by this approach. The second approach is to replace text-based passwords with another cognitive approach such as graphical passwords, or with alternative schemes such as biometrics, smart cards or the adoption of SSO. However, these types of authentication approaches require server-side changes in the existing authentication techniques by web developers and administrators. The last category of approaches to solve the password problem is to aid the user with the use of technology such as password manager applications.

Password managers are programs that typically store and manage all passwords in a location that is protected and accessible with one master password, using encrypted methods in order to eliminate the burden of remembering multiple passwords. Besides, this tool supports the use of a strong unique password for each site, thus enabling a reduction in password reuse. Unlike other alternative solutions to text-based passwords, password managers are an easy-to-adopt approach since they can be integrated with the existing authentication methods used on the server side.

2.8.1 Additional features of password managers

Further to the management of account credentials, many of the available commercial password manager applications are provided with some additional useful features.

- **Synchronisation.** Due to the fact that users currently tend to access their online accounts from more than one computer device in a typical day, such as mobile devices or a home/work desktop or laptop, many password managers support authentication with stored passwords from other different devices. These tools allow synchronisation of stored data automatically, usually through a cloud service.

- **Backup.** Aiming to satisfy users' concerns over losing their data and thus increasing their trust in the use of a password manager, some of these tools provide an option for exporting the saved data, and creating a backup that can be stored offline. Users can use the backup for import back into the same password manager or another competitor.
- **Password generator.** As password managers exist to mitigate password weakness caused by human cognitive limitations to cope with unrealistic password requirements, many password managers offer some features to improve the security of end users' passwords. One of the common features is to generate strong passwords that typically consist of random characters. Some password managers allow the user to be involved in the creation of these random passwords by providing some parameters to control the characteristic of the generated password, such as the length and the character classes. Furthermore, aiming to increase the usability of the randomly generated password, some of these tools offer a pronounceable password generator that might be easier to recall and type.
- **Auto-filling login data.** One of the main usability issues of passwords is typing a secure password into the login screen. Since a secure password is ideally randomly generated, it is not familiar to the users, making it a burden to type it. This problem is more serious when users use a mobile phone device to enter their password. Therefore, many password managers offer a feature to automatically fill in the login credentials when the user wants to access their accounts. Other password managers provide a manual method to enter the credentials by copying and pasting the required login data.
- **Safe sharing.** Users often share information with others, such as a partner, colleagues or children. These data range from contact information, insurance number and passwords to even credit card data. While sharing sensitive data might be necessary, it creates a threat that may pose a serious risk. Many password managers let their users share and transfer passwords or other data securely in an encrypted format. Moreover, some password managers allow their users to revoke sharing whenever they want.
- **Changing passwords automatically.** One of the pieces of password security advice that web users always encounter is to change their passwords periodically; typically every three months. While changing passwords can protect the accounts from being hacked, this advice is often neglected by end users due to the usability cost of applying it. Some password managers offer a feature to change the stored passwords on a regular basis automatically, to ensure the security of the passwords without bothering the users.
- **Storage for other sensitive data.** Although password managers were originally designed for storing login credentials for online accounts, many password managers currently provide storage for other data such as Wi-Fi passwords, bank details or security notes. Fur-

ther, some password managers support storage for other types of data besides text, such as audio, video or photo.

- **Access control.** Since password managers have the passwords to many users' online accounts, they are an attractive goal for attackers. Thus, many password manager developers apply methods to protect these tools. One of the commonly applied methods is 2FA. So, in addition to the master key (i.e. the password/key used to access the password manager), the users are required to provide an additional secret such as OTP or their fingerprint. Some password managers have added an additional security measure by allowing their users to restrict the access to their data to certain IP addresses or specified countries.
- **Auditing.** Trying to increase the trust level in using password managers, some of these tools audit the access request and log in information each time the storage is accessed. This information might contain the access time, location, or the device used. The audit log is sent to the user's email or recorded on their password manager web account.
- **Security assessment feedback.** Another feature that is provided by some password managers is monitoring the users' passwords to measure their quality and notifying them with proper security feedback. The feedback can appear at the time of creating the passwords by flagging up a weak password or using a password strength meter. Also, some of these tools give an overall security assessment of all the stored passwords and detect reused ones.

2.8.2 Types of password managers

There are many password managers available commercially. Generally, there are three non-distinct types of password managers: the first type can be found in web browsers as a built-in browser function that allows a user to save a password that has been entered while using the browser through a pop-up dialogue box. Examples of browsers offering this type are Firefox, Google Chrome and Internet Explorer password managers. The second type is available as a browser extension that requires installation by users on their web browsers. The third type is the dedicated or stand-alone password manager. However, most of the dedicated password managers are also available as a browser extension. In terms of the password manager storage model, these applications fall into the following categories:

- **Local-based password manager:**

This type of password manager application lets users store their sensitive information locally on their own computer device or on a portable device such as a mobile phone or a USB flash drive. An example of this type of password manager is KeePass, which is an

open-source password manager that encrypts passwords with either a master password or a key file.

- **Cloud/web-based password manager:**

Unlike local-based password managers, cloud password managers store users' passwords on the cloud and users authenticate to access their passwords. Many cloud password managers are commercially available, such as LastPass, which encrypts and decrypts the passwords on the client side using a master key. Some of the available password managers give their users the option to save their passwords either on the cloud or locally on their own devices.

- **Password manager that does not store any passwords:**

This is also known as a 'hashing password manager'. It avoids the need to store encrypted passwords. It uses hashing techniques to derive random passwords from a hash of the master password, the username, and the domain name of the website. Examples of these types of password managers are PwdHash [203], SuperGenPass [257], and Passpet [211].

2.8.3 Adoption of password managers

Despite the availability of different types of password managers, these tools are not widely adopted.

In a survey by Hoonakker et al. [2] to understand users' password behaviours, they found that only 1% of the participants reported that they used a password manager. Similar to this result, Stobert and Biddle [6] asked 22 users, in an interview study, if they used any kind of password manager, and no one reported currently using a dedicated password manager application. Ur et al. [56] conducted a think-aloud lab study with 49 participants to understand users' misconceptions about password strength and the strategies and inspirations of their common password patterns. They found that only two of the 49 subjects reported that they used a password manager. Wash et al. [30] conducted a study to understand actual online password behaviours using web browser plugins. They found that 26 of the participants (19%) had a browser-based password manager enabled during the study.

Zhang-Kennedy et al. [67] conducted two studies to assess the effectiveness of using visual communication for understanding password-guessing attacks. Their study revealed that only 10% of the participants in the first study (2 out of 21) reported that they used a password manager, and in the second study, ten users out of 55 (18%) said that they used a password manager. Das et al. [106] conducted a survey to understand users' behaviours in password construction across different online accounts. They found that only 6% of 224 participants reported that they used a password manager.

2.8.4 Password-manager-related works

Because of its potential to ease the password burden and alleviate weakness, password managers have enjoyed much attention from researchers in the last decade. However, most of the existing work on password manager has focused on the technical side of these tools. The aim was to improve their security and usability by proposing novel password managers or evaluating their security, usability or both. Less work has been done to understand the human perspective related to adopting and using password managers. Different studies have been conducted, aiming to improve the security of password managers by proposing new password manager applications or analysing the security of existing tools.

Ahuja et al. [50] proposed an Android password manager application that provides an extra layer of security. The proposed password manager uses an image to store all login credentials instead of using the typical database. It takes login data (email address & password) as input from the user and then encrypts them using a Blowfish algorithm. Finally the encrypted data is stored inside an image selected by the user using the Least Significant Bit technique.

Wang et al. [52] proposed Amnesia, a bilateral generative password manager. It generates the requested website passwords for the user using both the master password and a secret information on the user's smartphone; thus, that is not vulnerable to password database leakage. They evaluated the proposed password manager and found that it increased password security while maintaining reasonable usability.

Research on the security of password managers has revealed some vulnerabilities to attack. Most of these studies theoretically analysed the security of these applications, focusing on cloud-based password managers [89,90].

Zhao et al. [89] analysed the security of two popular cloud password managers, LastPass and RoboForm. They investigated the security design and implementation of these two tools focusing on three types of attacks: brute force, local decryption, and request monitoring attacks. The study identified some security risks, such as the vulnerability to server-side monitoring capability and local decryption attacks. The authors provided suggestions to improve the security design of these two cloud password managers and similar systems. In the same vein, Li et al. [90] analysed the security of five existing cloud-based password managers and identified some key security concerns with these tools. These includes: stealing the master credentials by spoofing the authentication dialog and leaking credentials into untrusted pages when using bookmarklet. Silver et al. [4] identified a number of vulnerabilities with the auto-fill policies of ten password managers across different platforms. These researchers found that the attacker could exploit these flaws in the auto-fill feature to extract passwords stored in the password manager, without interacting with the user, in the context where the user is connected to the Internet using an access point such as a Wi-Fi hotspot. Although the researchers found some vulnerabilities in password manager tools, they concluded that the risks could be mitigated and using these

tools helps to strengthen credential security rather than weakening it. Furthermore, passwords of users who use password managers can be more secure than those who choose to use coping strategies to recall and type their passwords [4].

Using digital forensic investigation techniques, Gray et al. [88] analysed the security risk of local-based password managers KeePass, Password Safe and offline- RoboForm. Their study revealed some risks that can make these tools vulnerable to attack.

Few scholars have focused their research on investigating and improving the usability of password management software. One of the few first studies considering the users' perspective of using a password manager was conducted in 2006 by Chiasson et al. [86], who studied the usability of two desktop password managers: PwdHash and Password Multiplier. They found that both of these tools had significant usability issues. The lack of feedback makes the participants confused about whether they have successfully activated the tool or not. Therefore, they suggested that greater visibility would enhance the usability of these tools. Further, more participants had incorrect or incomplete mental models about how they worked. The poor mental model, together with the usability issues, affected the participants' ability to use the password manager securely. While this study aimed to test the usability of two specific password managers, it provides a baseline from which to consider the user perspective when designing these tools. In 2010, Karole et al. [87] conducted a comparative usability study between three password managers: (LastPass) online, (KeePassMobile) mobile phone and (Roboform2Go) USB password managers. Interestingly, they found that although the online password manager was the easiest to use, users preferred to use the other two portable password managers. Particularly, non-technical users who participated in their study preferred the phone password manager to the other types of password managers. This was due to the fact that users were not comfortable giving control of their passwords to a remote entity because of security and privacy concerns and they preferred to manage their passwords themselves on their own smartphone device that is always present with them.

Schougaard et al. [85] evaluated 14 cloud-based password managers against some functional and non-functional requirements that a cloud password manager service should have to improve performance, usability, or reliability. For example, having a distributed password database and supporting 2FA for functional requirements, and having an open-source licence and giving users the option to store their passwords where they have control for non-functional requirements. They found that none of the password managers fully satisfied all of the tested requirements.

Barbosa et al [49] designed UniPass, a password manager for visually impaired users based on a smart device using QR codes and high-frequency audio tones. They evaluated the usability of UniPass compared to two existing password managers LastPass and StrongPass. They found that participants took the shortest time to log in when using UniPass. Furthermore, they suggested that password managers are a promising approach to web authentication for visually impaired users.

Many password manager applications have been proposed and developed by security experts. Moreover, researchers in computer and information security have paid attention to exploring and improving the security of these tools. So, it seems that password managers are a promising tool - at least in the current era- for providing a realistic solution to the password problem. However, it is not clear to what extent these tools are accepted and adopted by end users, which suggests the need for human-centric research to investigate users' perspectives about using password managers.

2.9 Conclusion

Most of the proposed techniques to improve textual passwords are not usable or secure enough to solve the password problem and they still have the usability problem that compromises security. Also, most of the studies on password creation and behaviour have only considered the desktop computer context and have often neglected the impact of soft keyboards on password creation and other relevant password behaviours. Soft keyboard is a representation of a physical keyboard shown on a touch sensitive screen. Other techniques to replace the textual password are either expensive to apply, as in the case of graphical passwords or 2FA, or not widely applicable, such as a SSO.

Password management systems seem a promising approach to improve password security while supporting usability. However, these tools are not widely adopted. Most of the existing research into these systems only considers the technical aspects. Less attention is paid to the human side, especially the factors impacting the adoption of these tools. The research reported here considers the human aspects of password manager adoption by smartphone users; aiming to understand and encourage the adoption of these systems. Techniques of human motivation have been applied in various fields of research, including education, gaming and health, in order to change people's behavior (refer to Chapter 4 for more details). Therefore, it has been decided to harness human motivation techniques, in a suitable intervention, to encourage the adoption of password manager.

Chapter 3

Password Manager Adaption Stages: An Exploratory Investigation Study

3.1 Introduction

Password managers are a promising solution to the current password problem; yet, they are not widely adopted. Little is known about the reasons for this phenomenon. It was decided to explore and understand user perceptions about adopting password managers, in the hope of identifying strategies to support their adoption.

Data were collected from two sources: (1) reviews from the Google Play Store and the Apple store for two popular password managers and (2) an online survey. The purpose of using the former source was to investigate the perceptions of password manager adopters, whereas the latter helped to understand the perceptions of people who may not yet have adopted a password manager, and could therefore explain the reasons that impeded this adoption.

Some findings were unexpected. Many users were not aware of the existence of these tools. Users need to have sufficient information about these tools before they will consider using them. The collected data was analysed using Grounded Theory and some important patterns of password manager adoption were identified such as the awareness of password manager and the intention to use it. A password manager application life cycle was defined, which shows the stages during the adoption process. This sheds light on the gaps in adopting password managers. The development of this model is described and some recommendations to encourage the adoption of password managers are suggested.

In the following sections, the methodology is described, followed by description of the data collected. Section 3.4 presents the qualitative analysis in detail. Section 3.5 uses an example to demonstrate the developed stage theory. Then, some implications are suggested before the conclusion.

3.2 Study Approach

To investigate the current adoption status of password managers and to identify the different factors impacting the adoption, or rejection, of these tools, two types of data were collected:

1) Reviews from application stores representing the opinions of users who chose to trial password managers. This enabled a preliminary investigation to help to understand why users use smartphone password managers. Two popular password manager applications, namely LastPass and 1Password [154] [156] were selected, based on the number of downloads and users' reviews. Then, user reviews of these applications were collected. A similar approach was used by [146] and [147] to reveal users' perceptions of applications in Google Play and Apple stores.

2) An online survey gathering 352 responses related to password manager use, exploring factors that encourage or discourage password manager adoption. An open-ended questionnaire was designed and validated by testing it with 34 randomly selected testers. Ethical approval was granted by the College of Science and Engineering at the University of Glasgow. Using an online survey allowed responses to be elicited from users worldwide and it afforded anonymity to offset social desirability bias [148]. To avoid incomplete participation due to fatigue, a maximum of five questions were used. To encourage disclosure, no identifying information or demographics were collected. The questions can be found in Appendix A.

This methodology was chosen to gather a range of data about users' perceptions of password managers from both those who had tried a password manager and those who might not have tried it. A step-by-step qualitative analysis was conducted on the collected data using the Grounded Theory analytical approach. This approach aims to develop an explanatory theory from important concepts emerging from qualitative data. It has been successfully applied in human computer interaction studies to elicit user perceptions on security and privacy when interacting with technology [1], [150].

According to Grounded Theory, a theory is defined as:

“a set of well-developed categories (e.g. themes, concepts) that are systematically interrelated through statements of relationship to form a theoretical framework that explains some relevant social, psychological, educational, nursing or other phenomenon .” (p.55) [143].

3.3 Data Collection

Data was collected from two sources: 120 online reviews and 352 responses from an online survey. Users' reviews of two popular password manager applications, namely LastPass and

1Password, on Google's Play store [151], and the Apple store [152] in three countries (the UK, US and Saudi Arabia) were collected. LastPass was chosen to represent a cloud-based password manager and 1password represents users' reviews about local-based password manager applications. The choice of three different countries meant that different populations of users could be included to uncover region-specific usage patterns, and these three countries were chosen to reflect countries at different stages of technological development. More specifically, The U.S and the U.K were chosen due to their status among the most developed countries while Saudi Arabia was chosen due to its status as an important developing country that persistence to become a greater competitor to advanced countries in the field of technology. The idea was to use the most recent 20 reviews for each of the two password managers in each of the two stores. Reviews in Google Play can be sorted by date, helpfulness or rating. It is recommended to have a minimum sample size of 20 for each culture measure in [153]. Surprisingly, in the Saudi Arabian store, no reviews or ratings were found for either application. Although this does not mean that these applications are not used in Saudi Arabia, it might suggest that users do not as readily review applications. It also gives an initial indication of the popularity of password managers, as compared to other types of applications such as messaging apps. The latter are highly rated in the Saudi Arabian App store. In the end, 120 user reviews were included in the study.

An open-ended questionnaire was posted in April 2016 via Google Survey. Participants were recruited using a snowball sampling methodology, via email and social media such as WhatsApp, Facebook, Twitter and Path. The snowball sampling is a method where research participants recruit other participants for a study. 370 responses were received; 3 were incomplete, 4 skipped 1 question and 11 were either invalid or the respondents clearly did not engage with the survey. After excluding these responses, 352 usable responses remained.

Based on the online survey, the spread of password manager usage was investigated. Although this was self-reported, 62 respondents (17.6%) said that they used a password manager application on their phone. However, only 24 of them (6.8%) provided the name of a dedicated password manager application; the rest either misunderstood the question or used methods other than dedicated password managers. About half of the smartphone password manager users (32) misunderstood the term 'password manager application' (even though a brief description was provided at the beginning of the questionnaire). Some thought it was the screen lock mechanism. Two respondents used their mailbox and notepad as a tool for managing passwords. Four users stated that they used the Google Chrome password manager. While Google Chrome can overcome the password memorability issue, it constitutes a big threat due to the fact that such passwords are easily accessed, in the clear, to anyone who accesses the device (Google recently required a password to show the stored passwords in plaintext). However, it has no integrated feature to generate a random password when signing up for a new website. The use of this memory aid might prevent the adoption of a secure password manager. Usage was low; although it

was somewhat higher than that reported by Hoonakker [2], given the fact that almost a decade has passed, the increase is paltry.

3.4 Qualitative Analysis

Because the study is an exploratory in nature, it is expected to be unstructured, qualitative study[51], focusing on collecting a wide range of data [116]. Therefore, the collected data from both the survey and the reviews was used together for qualitative analysis. The Grounded Theory methodology has been chosen for the qualitative analysis because it is suitable for research fields that have not been widely explored and it provides an opportunity to generate new theories and research directions [144]. Based on this approach, the analysis process consists of three basic steps. The first step is open coding, breaking the collected data into meaningful units and assigning a descriptive code to each. Then, the codes are categorised into themes in the axial coding process. The last step is a selective coding process, placing the axial codes into a 'big picture' that refines it into a theory.

3.4.1 Open Coding

This is the first level of data analysis: the process of analysing the data to extract thoughts, ideas, and meanings encompassed in the text. It begins by breaking the text into meaningful units (such as sentences) and then examines the text unit-by-unit and assigns a descriptive code to each unit.

To estimate coding reliability, a second coder independently coded 12 reviews and 37 responses from the online survey. The resulted codes were compared to the initial coding and discussed until agreement on the meaning of each code was reached. The final codebook was used to code the remaining data. Then, the second coder used the codebook and coded a random sample of 24 reviews and 70 survey responses. Inter-rater reliability was calculated using the percentage-agreement method, and was found to be 0.93.

One of the codes was 'I am already secure', and it was used when participants indicated that they did not see the need to use a password manager because they already felt secure using their current management method. This feeling of security can be due to the use of second factor authentication:

*"I don't feel I need it [the password manager]. I use one-time password applications and I believe it is secure", [Survey-P149].*¹

However, some participants thought their current password management methods were secure:

¹[data source: Survey or review - Participant number]

“I use one strong password for everything ”, [Survey-P52].

The number of passwords that the users owned was revealed in two different situations: it was mentioned as a reason for using a password manager in some reviews and it was also mentioned as a reason for not using a password manager in the online survey.

“Being an IT/Network Administrator, and having to remember over a 100 different logins and passwords, this thing is a life saver” [P3-1Password Review-Android].

“I have a few passwords to remember so I don’t need an external help” [Survey-P88].

Since these two conditions are different in terms of how they influence the user’s decision to use a password manager or not, they were coded using two codes. The first code was ‘Having few passwords’, which described the opinion that the user did not need to use a password manager because they had only a few passwords. The second code was ‘Work demand’ and it was used when a participant indicated that the nature of their work demanded a large number of passwords.

3.4.2 Axial Coding

This coding process identifies relationships and/or themes among the open codes, finds the connections between them and organises them into meaningful categories. This process began by writing the open codes on Post-it notes and sticking them on to the wall (Figure 3.1). Then they were organised and reordered, aiming to find connections and relationships between them. All the open codes that emerged from open coding are listed in Table3.1. A description of each open code is also presented in the table. The open codes are grouped into categories that show the result of the first round of axial coding.

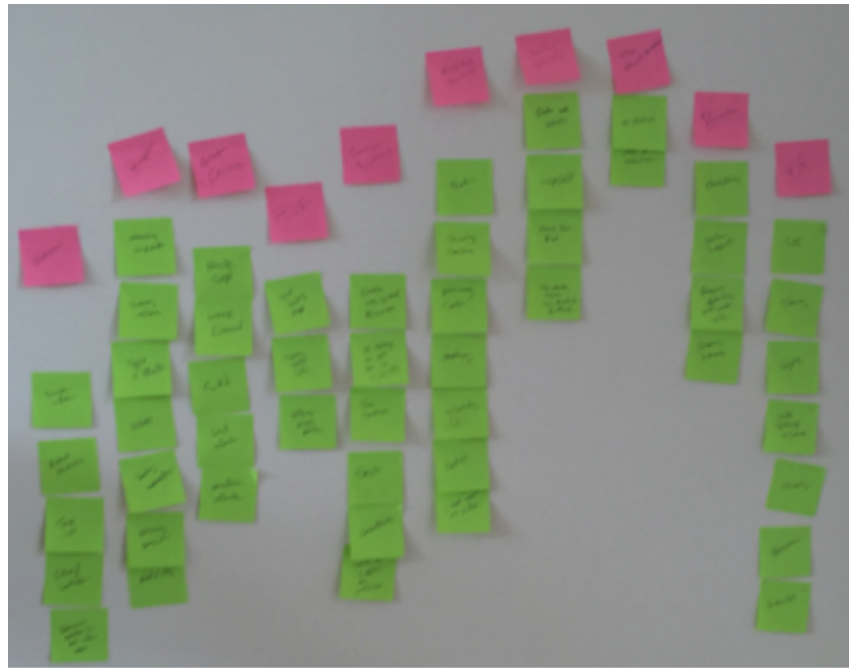


Figure 3.1: Arranging the codes in the axial coding process

Table 3.1: The codes used in the open coding stage grouped by the initial axial coding categories

(PM=Password Manager)	
Code	Description
Awareness:	
•No awareness	→Not aware of the existence of PM tools.
•Lack of information about it	→Poor awareness of how it is implemented how to use it or the advantages of using it.
No need :	
•Data not valuable	→Considering their data not to be valuable.
•Insignificance	→Users did not see the need to have strong passwords as they believed that their online accounts would not be attractive to attackers.
•Having few passwords	→The number of passwords affected the decision to adopt a PM.
•I am already secure	→ Users did not see the need to use PM applications because they believed that their current password behaviours were secure.
•Memory Mastery	→ The users described their ability to remember their passwords or their desire to challenge themselves by retrieving the right password from their memory.
Psychological concerns :	
•Trust	→Generally, not trusting the PM to store passwords.
•Privacy concern	→Feeling that PMs can,expose,passwords to others.

Table 3.1 continued from previous page

Code	Description
<ul style="list-style-type: none"> • Security concern • Risk • Uncertainty/lack of technology knowledge • Control • I don't want to use it first 	<p>→ Feeling that PMs can be hacked.</p> <p>→ Describing the fear of the risk of using PM on a smartphone device to manage passwords.</p> <p>→ The lack of certainty or the limited knowledge of PMs makes the user reluctant/unconfident to search choose or use a PM.</p> <p>→ The concern about not being able to maintain control over the passwords when using a PM.</p> <p>→ Waiting for the app to be popular because participants did not want to be the first to take the risk of using a PM tool.</p>
Contextual factors:	
<ul style="list-style-type: none"> • Device resource limitations • Time constraint • Cost • Connectivity • Lack of support from other services 	<p>→ Limitations in phone resources like battery, memory or processor prevent users from using PMs.</p> <p>→ Do not have time (or less willing to spend time) to consider using a PM finding one or setting it up.</p> <p>→ The cost of using a PM (monthly subscription or one time payment).</p> <p>→ The availability and the quality of the internet connections.</p> <p>→ The lack of support or PM features (such as the auto-fill feature) from other service providers such as web browsers websites or mobile apps.</p>
Negative features:	
<ul style="list-style-type: none"> • Linkage with other 3rd party services • Country-specific features • Differences across platforms 	<p>→ Complaint about having to use an additional account or app to perform a function such as sync.</p> <p>→ Criticism that the interface is customized for a particular audience.</p> <p>→ Complaint that the interface and or the provided features are not supported or are different across different devices/platforms.</p>
External influential factors:	
<ul style="list-style-type: none"> • Experience hacking • Work demand • Subjective norm • Social and media influence 	<p>→ The fear of or the experience of account hacking.</p> <p>→ Users need to accomplish their work and deal with many accounts and passwords.</p> <p>→ The social pressure to use a PM.</p> <p>→ The influence of media such as podcast and social influencers such as experts or family members on the adoption of a PM.</p>
Vendor-related factors:	
<ul style="list-style-type: none"> • Transparency • Communicating with users 	<p>→ Publicity of relevant information of PMs such as the source code or explaining how a hacking incident has occurred.</p> <p>→ The communication with customers through media and the support delivered made a good impression.</p>

Table 3.1 continued from previous page

Code	Description
<ul style="list-style-type: none"> • Regular updates to meet users needs • Vendor specialisation 	<p>→Regular updates and continued improvements to fix flaws, improve usability, and introduce new features.</p> <p>→Indication that the PM developers are trustworthy.</p>
Positive impact:	
<ul style="list-style-type: none"> • Memory support • Time saving • Typing effort amelioration • Access • Improving security • Privacy preservation • Availability • Password security 	<p>→Support the memory.</p> <p>→The use of a PM saves time.</p> <p>→The difficulty related to entering a secure password when using a phone is ameliorated when using a PM.</p> <p>→Using PMs ensure users are not locked out of a website and they can access their accounts from any other device.</p> <p>→The use of a PM increases the security level of users online accounts and makes them feel secure.</p> <p>→Privacy is respected by the developers of the application.</p> <p>→Users' satisfaction of having their passwords and important documents available any time.</p> <p>→The use of PMs improve the strength of the generated passwords.</p>
Positive features:	
<ul style="list-style-type: none"> • User interface • Synchronization • Safe password sharing • Secure storage. • Usability • Browser • Auto-fill • Two-factor authentication 	<p>→The design of the interface is simple and uncomplicated.</p> <p>→Synchronizing passwords between devices.</p> <p>→Safely sharing passwords and important documents with other users.</p> <p>→PMs provide security storage for different types of data. such as documents.</p> <p>→Describing the ease of using a PM.</p> <p>→The availability of browser extensions or the integration of a browser in the application itself.</p> <p>→Filling-in the login credentials automatically.</p> <p>→Describing the use of two-factor authentication to access PMs.</p>
Behaviour:	
<ul style="list-style-type: none"> • Gathering information • Rational evaluation • Temporary use • Deleting PM • Password behaviour 	<p>→Searching for information about PMs. e.g: asking, reading or exploring via web.</p> <p>→Describing the decision process of whether to install a PM or not.</p> <p>→Temporarily trying a PM before using it.</p> <p>→Deleting a PM or switching to another PM.</p> <p>→Describing how the PM is used to manage passwords/accounts.</p>

To support axial coding, an 'Ordering' process has been suggested in which an ordering family is used to identify relationships between phases, stages and/or consequences. There are three ways of ordering: structural, temporal and conceptual [145].

Generally, the emergent codes fall into two main categories: 'before using a password manager' (such as Lack of information and Insignificance) and 'after using a password manager' (such as synchronization and time saving). Therefore, a temporal ordering was identified. The previously identified themes were grouped into more general categories following the identified order. These categories are explained in the following sections.

Awareness

If users are not aware of the existence of password managers, they will not think of using these tools. In the survey study, many participants reported not being aware of password managers. Some examples of their responses are:

"I have no idea about their existence" [Survey- P82]

"I did not hear about it before" [Survey-P173]

In the analysed data, the users mentioned a number of sources through which users can be made aware of these password management tools. The media, such as podcasts, can influence users to attempt to use a password manager. For example:

"What convinced me to try it was the Mac Power Users' podcast #173 where they spent the whole hour on how useful 1Password is. Listen to that show and you will appreciate this app " [P6-1Password Review-IOS-U.S].

Also, having those close to the users interact with them directly also has an impact:

"My husband encouraged me to download this app " [P4-1Password Review-IOS-U.K].

" I've recommended it in person to countless friends and they use and love it " [P10-1Password Review-IOS-U.S].

"Got multiple friends and family members to use their service" [P3-LastPass Review-Android].

Intention to use a password manager

After people become aware of password managers, they might be interested in using them. The study reveals some factors that influenced users' interest in adopting a password manager.

One of the strongest reasons for adopting these tools, according to both survey respondents and reviewers, is the password security and memorability issue. The fact that many users possess increasing numbers of accounts makes it a challenge for most of them to construct unique and

secure passwords and remember them. Password managers can help their owners to construct strong passwords, instead of trading off between memorability and security. This encourages the adoption of password manager applications. Here are some examples:

“ I used to have a single password for all of my secure sites due to the hassle of trying to remember multiple ones. Then I discovered Lastpass. This makes logging into all of your secure pages simple and hassle free. No longer do I have a single password, in fact, every password I have now is so complex, even I can’t remember it. The only password I need to remember now is the Lastpass one itself” [P14-LastPass Review-iOS-U.K].

“ It’s an incremental life-changer that actually lets you have stupid-complex passwords without having to remember them all (or use the same one over and over)” [P5-1Password Review-iOS-U.S].

“ Now, instead of agonizing over a password I can remember vs. one that’s secure, I am able to choose secure every time ”[P7-1Password Review-iOS-U.S].

Some users referred to memory-related reasons for adopting password manager applications:

“ Because I always forget my passwords” [Survey-P224].

“ I use a lot of different passwords that I forgot after a while or when I have to change the password to another, I keep remembering the old one not the new one” [Survey-P241].

“ My passwords are different for each account and difficult to remember them” [Survey-P154].

“ For me, it’s a great tool not having to remember numerous login details” [P3-LastPass Review-iOS-U.K].

“ I was struggling to remember all the different passwords I had at all the different websites I visited ” [P4-1Password Review-iOS-U.K].

They said it helped to retrieve infrequently used passwords:

“ I’m no longer reluctant to create accounts for things I only rarely look at (because I don’t have to worry about remembering login credentials and passwords); I never have to try to remember what I used for security questions and answers (because I record all of that into OnePass)” [P10-1Password Review-iOS-U.S].

Or passwords that were used years ago:

“ If you’ve ever found yourself staring blankly at the "security questions needed to verify identity" password reset prompt, because you have absolutely no clue what your favourite food was 8 years ago, then do yourself a favour and download Last-pass” [P8-LastPass Review-Android].

In addition, some reviewers reported that these tools eliminated the need for fallback authentication when they forgot their passwords:

“ Even those ridiculous fallback questions (what’s your favourite movie... Like that’s never going to change!). Even for my "mother’s maiden name", I use secure random strings, unique per site, on most sites” [P7-1Password Review-iOS-U.S].

One of the reviews referred to the difficulty related to entering a secure password when using a phone, which emphasises the importance of using supportive tools, according to the reviewer:

“ shudder to think what it would be like to type an actually secure password on one of your phones ” [P3-1Password Review-iOS-U.S].

One of the reviews emphasised the role of subjective norms, i.e. the perceived social pressure to engage, or not to engage, in certain behaviours. In terms of influencing people to use password manager applications:

“ In fact, it’s not just about you, but about your family, friends, and colleagues. Have you considered that when your computer, mobile device, or online accounts are stolen or hacked that you may be exposing information about your family members, friends, and colleagues? Well, the truth is, you are ” [P20-1Password Review-iOS-U.S].

Moreover, password managers saved people time that had previously been spent on logging in manually:

“ go read a book or something with all the free time you now have” [P3-1Password Review-iOS-U.S].

In some reviews, users stated their need to accomplish their work on time, which requires them to deal with many passwords, and they found it helpful to use such applications. For example:

“ Being an IT/Network Administrator, and having to remember over a 100 different logins and passwords, this thing is a life saver” [P3-1Password Review-Android].

“ this app has been essential for my day to day work with my 130 something logins ” [P9-1Password Review-iOS-U.S].

“ If you’re like me, then you have 50+ login credentials throughout the Internet ” [P16-1Password Review-iOS-U.S].

“ It has truly kept me from losing my mind due to the amount of passwords stored in my head ” [P4-LastPass Review-iOS-U.S].

A couple of reviewers stated that their experience of previous attacks influenced them to start using password manager applications:

“ the headache that comes with it, as happened to me after my email address and password were kindly hacked into by someone in China and displayed online along with the other 300 000. I only found out by curiosity in searching for my email address” [P3-1Password Review-iOS-U.K].

“ It was literally just by sheer luck that I captured it before it happened. I used similar passwords for almost everything and let a colleague type in my password on my office PC while I was in the middle of something else. Big mistake. He "jokingly" logged onto my Twitter and Facebook accounts and put up comments without my knowledge. Although it was a joke to him and I wasn't upset, it made me think, so the following day I downloaded LastPass and changed all my passwords to 256 bit AES encryption” [P12-LastPass Review-iOS-U.K].

A number of participants who do not use password manager applications indicated that they might consider using them if they knew that other users were doing so:

“ If many people use it first without problems”,[Survey-P339].

“ if it became popular and many people use it without any issues”,[Survey-P319].

Or if it was suggested by others:

“ suggested by close friends”,[Survey-P157].

“ friends recommendations”,[Survey-P103].

However, some users in the study were less interested in using a password manager. The participants reported several reasons behind the low intention to use. Some users expressed the opinion that they did not need to use password manager applications because they believed that their current password behaviours were secure:

“ I use one strong password for everything”, [Survey-P52].

Or they used other security tools, such as one-time passwords:

“ I don't feel I need it I use one-time password applications and I believe it is secure”, [Survey-P149].

In addition, some participants were confident in their ability to remember their passwords:

“I don’t need it, can remember my passwords”, [Survey-P209].

“I can remember my passwords I use. And I would not feel safe with all passwords saved accessible through just one other password”, [Survey-P342].

Some preferred to use the fallback authentication recovery function in the case where they forgot their passwords, instead of using a password manager:

“Because I rarely forget my passwords, also I prefer if it happened and forgot the password to reset it”, [Survey-P315].

Moreover, some participants believed that they did not need these supportive security tools because they were already taking online protective action by visiting only what they believed to be trusted websites:

“Because I do not think I need it. I visit only popular websites so I do not need very very complex password for them”, [Survey-P290].

However, some participants considered themselves to be secure. Here are some examples demonstrating that people thought using the same password for many accounts was secure behaviour:

“I didn’t need it yet. I always choose the same password. I am good at memorising numbers and codes”, [Survey-P17].

“I have one password for all my accounts. I don’t need to write it”, [Survey-P249].

“I don’t feel like I need it. I use strong passwords by myself and they are very similar, so I don’t get confused”, [Survey-P285].

Other participants did not see the need to use password manager applications because they did not have many online accounts:

“I use to memorize my password since I don’t have too many”, [Survey-P331].

“Also, I have a few passwords to remember so I don’t need an external help”, [Survey-P88].

Some participants considered their data not to be valuable:

“No reason I do not have anything to worry about I do not want to bother myself with complicated passwords”, [Survey-P314].

“I have not got important things on my mobile”, [Survey-P343].

“Maybe if have important accounts like a bank account”, [Survey-P331].

Other participants did not see the need to have strong passwords, as they believed that their online accounts would not be attractive to attackers.

“If I get rich or became a politician then I would think about strong passwords”, [Survey-P314].

“I believe that it is too much for me to have such applications, as I am not a celebrity or politician and therefore have no stalkers”, [Survey-P295].

As password manager is not widely known to smartphone users, many thought it was a recent development and they thus did not want to be the first to take the risk in using such applications:

“Not that popular so it must be not that good”, [Survey-P189].

“If I see many people use it and like it or famous people use it and like it”, [Survey-p189].

Some participants attributed their decision to not use a password manager to their desire to challenge themselves by retrieving the right password from their memory.

“I like to challenge myself by remember my passwords.. feel proud of myself it's not a joke! ”, [Survey-P95].

“I do not like to depend on technology to remember all my passwords This will make my memory lazy”, [Survey-P93].

While many password manager application users believed that these applications maximised their online security, those who chose not to adopt these tools had concerns about their security:

“I always feel that the security of these applications are not good ”, [Survey-P243].

“I do not fully trust that the software will be able to provide enough security. After all, there is no such thing as an impenetrable security, especially in digital world. Should someone hack into my account, they will know all my passwords. Even though there is a risk that I will not be able to remember some of the passwords, then at worst, the data will just be lost”, [Survey-P256].

Particularly concerning was the fact that these types of systems have a single point of failure:

“Risk of keeping all eggs in one basket”, [Survey-P303].

“Maybe because when the attacker can get inside the password manager, he/she can take all my passwords. But when attacker get one password and get inside my email that will be more secure because I only lose the access to my email account only not all accounts”, [Survey-48].

“It is a risky application if master key is attacked then every thing gets lost”, [Survey-P88].

“... its going to be easier for other people to hack my account since they can get the password from the password manager”, [Survey-P155].

They worried that these types of systems might attract attackers:

“I don’t like the idea of having all my passwords stored in one place (The password manager app) which will be most likely on the list of hackers to crack and if they already did crack it, it will obviously be the first thing they will look for after attacking my PC or Phone and that doesn’t quite feel safe, nor assuring. To me using a word document that doesn’t look like anything special feels safer and you can lock it with a password too”, [Survey-P207].

“I don’t trust applications. Hackers may use these kinds of applications to achieve their personal and illegal goals”, [Survey-P253].

There was concern about it landing up in the hands of another person:

“My accounts are very important to me and cannot trust putting them in danger of getting lost if my phone get damaged or stolen”, [Survey-P294].

“Because my cell phone is sometimes used by my children and other family members there is a risk to use it”, [Survey-P323].

Also, some participants believed that their phone itself was not secure; that it might have viruses that could affect their passwords if they used a password manager:

“It’s a security matter. I use it in my computer because it has anti virus and firewall and sometimes when I google a website it tells me which website is risky. My phone has non of these things and I have some applications in my phone games that I believe they are not very safe”, [Survey-P219].

“Cuz my phone got viruses and not safe”, [Survey-P324].

Also, they seem aware of the security risk of using public Internet services:

“ I use public Wifi networks which makes it much easier for attackers to attack my passwords if I use password manager application”, [Survey-P316].

In addition, users seem unsure about their current security knowledge and information and thus do not want to put themselves at risk of having yet another critical application to look after:

“ Advice on how to stay secure when using it”, [Survey-P316].

Some of those who chose not to adopt password managers cited the reason as being privacy concerns, such as a lack of trust in the vendors. For example,

“ personally I don’t know anything about the developers or the app source”, [Survey-P131].

“ I don’t trust these application. They made in U.S. to know everything about us. Now they know everything but not passwords so they made this application to trick us. If you see images of Google data centre you will not use these kinds of systems anymore ”, [Survey-P169].

“ I don’t trust it, as I am not sure about the developers of this app and what they can do with my details”, [Survey-P3].

Also, some stated that if they trusted the developers then that would make it possible for them to use these applications:

“ May be if it is: [...] from a trustful source”, [Survey-P82].

For example, if it is developed by a well-known organisation:

“ A password manager that is developed by popular companies like Google, Apple”, [Survey-P147].

“ If distributed by trusted source or big industry name like apple keychain”, [Survey-P131].

Or developed by people they trust:

“ Nothing will make me use it unless I develop it myself or someone trusted like people in universities”, [Survey-P169].

Others said if the application was open source, they might use it:

“ Open source code and easy to understand description”, [Survey-P252].

However, one of the reviews referred to the importance of trading off between privacy concerns and their security password behaviour:

“ This is not an app for nerds, geeks or those who overdramatise the importance of internet security. Put simply, if you care in any way for your personal privacy and / or the stuff you store and access online, you need to wise up, stop using the cat’s name for every password on every site you access, and download this app ”
[P2-1Password Review-iOS-U.K].

Search

After the users accepted the idea of a password manager in theory, the adoption process began with the user starting to search for a suitable password manager. The form this search takes depends on the users’ current knowledge and what they are looking for.

Some users search for general information about password managers to find out about the different features that can come with these applications:

“Investigating them in depth ” [survey-p344],
“ search about it in the web” [survey-P2] and
“ finding a good one” [survey-P348].

Some users mentioned that they would ask other users who they trusted what they knew about password managers:

“Friends recommendation” [survey-P103] and
“ask friends and experts” [survey-P2].

Other participants who seem aware of password managers search for a particular type of password manager, for example, a cloud password manager or open source:

“ the only cloud security solution to use. [...]. I searched and researched every solution available before implementing Lastpass” [P16-LastPass Review-Android]

Some participants mentioned that they searched for a password manager in the application store:

“I type password manager in the store and it shows some apps”, [survey-P6].

Other participants were not aware of the already available password managers and mentioned that finding a password manager with a particular feature would make them use a password manager:

“open source code” [survey-P252] and
“If the password is my fingerprint or something like that” [survey-P234].

The time constraint may hinder users from searching for a password manager and installing it:

“Having time to search for a perfect password manager” [survey-P352].

Also, the lack of technology knowledge could make the user uncertain about how to search for a password manager:

“I don’t know which one to trust” [survey-P232].

Table 3.2: Some of the main functionalities of Password Manager

Function	Meaning
Auto filling	Password manager can automatically fills login credentials (i.e. user name and password) ;eliminating the difficulties related to typing a secure passwords- especially when using a phone device.
Password generator	Password manager can, optionally, generate a complex password for each account and save them for the user. So the user can use secure passwords without having to remember them.
Secure storage	Some password managers provide a storage , as an extra security feature, for other types of data ; such as photos, notes or credit card information.

Decide

After users search for password managers, they might end up with a list or a number of choices of password managers. At this stage, users have to make a decision over whether to select one of the resulting password managers or reject the idea. Some participants described the struggle over deciding which password manager to choose:

“I have been thinking about getting one but I can’t decide which one yet”, [survey-P272].

Some users were rational in their decisions and described their trade-offs between password manager specifications:

“I don’t regret buying it and when I compare it with similar products on the market, it still seems to be the best available” [P15-1Password Review-iOS-U.K].

“I was debating between using LastPass or a KeePass/DropBox/KyPass solution. Both have their pros and cons, but this mobile app pushed me towards the KeePass side” [P15-LastPass Review-iOS-U.S].

The adoption decision might be made after reading reviews:

“After reading other reviews I decided to buy the OSX version and this app and haven’t looked back since” [P12-1Password Review-iOS-U.K].

Other participants mentioned that they decided not to install a particular password manager that they had chosen, based on rational reasons:

“I was about to use Dashlane (I think that is the name) last year and then it struck me that I could be in trouble if I could not pay the monthly fees”, [Survey-P350]

Try

When a user decides to install a password manager, he/she might start to try it and evaluate it. Based on their own experience, they will either continue to use it or uninstall it:

“If I tried it and liked it” [Survey-P347],

“I will try it by myself and see” [Survey-P190],

“Just a try” [survey-75] and

“for sure I will try it” [Survey-P77]

One participant mentioned trying two different password manager applications:

“I tried two of them but I could not use them ” [Survey-P116]

Another participant said that he/she tried a password manager and then deleted it due to a bad experience that consumed time:

“ I tried Ipassword and it took a long time so I deleted it.” [Survey-P86]

Some users stated that they had tried a password manager with only one of their accounts and said that they stored passwords for some of their accounts, based on their importance:

“I chose to save my account in Debenhams to try but it took ages for me to save it. The other accounts are private for me I can’t save them on an app that I have just known”, [Survey-P86]

“I’ve only downloaded it. I will add my Facebook account only just to try the application.”, [Survey-P4]

Long-Term Adoption

Based on the user’s experience of trying a password manager, they might continue using it in the long term to manage the rest of their accounts. The study shows some factors that influence users’ satisfaction with their experience with password managers.

Many reviews indicated that the delivered customer support made a good impression, as can be seen in this review:

“Their technical support truly listens to you. With most apps, you sometimes wonder if there is someone still on the other end. If there is any problem they will fix it” [P1-1Password Review-iOS-U.S].

“they responded within minutes! Their help was spot on correct, courteous, and quick” [P8-1Password Review-iOS-U.S].

In contrast, some reviewers who were unhappy with the password manager referred to poor communication with the service provider:

“contact support with a serious issue and they give you an unhelpful curt answer and when you try to follow up with a request for clarification they shut down the opportunity with a “status resolved” door slam in your face” [P20 -LastPass Review-iOS-U.S].

The reviews reveal that keeping in touch with users to provide transparent explanations of any security incidents could increase user confidence in the application:

“Security now also explained on a previous episode how LastPass was hacked; which calmed my nerves after listening to the episode” [P6-LastPass Review-Android].

Many reviewers were impressed with the different options and functions available. They reported that these apps had not only changed their password usage behaviour but also provided extra security features that made their lives easier:

“I have scanned and added many important documents such as birth certificates, auto insurance cards, social security cards, passports, drivers licenses, medication lists, banking info and much more. ALL of these items are available to me and my wife anywhere, any time with the touch of a screen, and they are all encrypted using 256 bit AES encryption” [P8-1Password Review-iOS-U.S].

“but it acts as a complete storage for everything important such as wallet items, router & server info, and much much more” [P9-1Password Review-iOS-U.S].

Due to security and/or usability requirements, the availability of the biometric fingerprint authentication mechanism seems to have had a big impact on the usage of password managers. While iPhone users rated 1Password because of the support of TouchID, some Android users complained about the lack of support for biometric authentication, especially those who had used 1Password on their iPhone or had migrated from iOS. For example:

“But there is no fingerprint support for Android. iOS version does have the fingerprint feature” [P20-1Password Review-Android].

Some users pointed out the advantage of having a password manager if one of their accounts is attacked, compared with the situation where they might have used the same password for more than one account. For example,

“I use 1Password multiple times a day to recall and fill one of my 1600 or so unique and ridiculously complex passwords. If someone gives away one of my accounts, it is zero panic” [P5-1Password Review-iOS-U.K].

“In summer 2014 when eBay passwords were compromised, I didn’t worry. My eBay password was unique to eBay so I knew my other accounts were safe. I simply changed my eBay password and went on with my day. OnePass makes this all possible ” [P10-1Password Review-iOS-U.S].

Also, they mentioned that password managers make them aware of password weaknesses:

“ Identify any password weakness or any password matching ” [Survey-P74]

Rejection

Based on the user experience, users might end up uninstalling the password manager:

“Tried and uninstalled” [P19-LastPass Review-Android].

“ It has been so frustrating I stopped using it” [P7-1Password Review-iOS-U.K].

In some cases, where users seem dissatisfied with their experience with a specific password manager, they deleted it and searched for an alternative password manager:

“ It is for this reason I have deleted the app and am now looking for an alternative provider of password storage!” [P9-LastPass Review-iOS-U.K].

“ I have now decided to look for alternatives, as this just does not cut it for me.” [P10-LastPass Review-iOS-U.K].

In other cases, users switch from one password manager to another one, if they were unhappy with their experiences with the former one:

“ Have been using Msecure password manager for years. Decided to try a change as Msecure was lagging in updates. Took the plunge and bought 1password.” [P20-1Password Review-iOS-U.K].

“ They do not allow you to recover your lost password. Therefore I did a lot of searching to find a good password app that has a lot of encryption and after trying too many to count, I found this one. I have been really happy with LastPass over the year that I’ve used it.” [P10-LastPass Review-iOS-U.S].

Table 3.3: The final axial coding

The code	Meaning
Awareness	The users' knowledge about the password manager.
Intention	The users' willingness to adopt a password manager application.
Searching	The process of searching for suitable password managers ; which includes the search for some desired features of password manager.
Deciding	The process of making a decision over which password manager to adopt.
Trying	The installation of a password manager in the user device. It might involves registering and trying the features of the password manager with few accounts.
Long-term adoption	The usage of password manager in the long term to manage passwords for different accounts.
Rejection	The uninstallation of a password manager.

3.4.3 Selective Coding

The final stage of data analysis in Grounded Theory is selective coding. This is the process of selecting the central or core categories that describe a phenomenon in the collected data, aiming to establish the basis for the Grounded Theory.

Through the analysis, a general theme about the sequence of stages that can develop in the adoption of a password manager emerged from the data. It has been noted that password managers, like organisms, have a growth imperative and are impacted by factors in their environments such as crowding, humidity, and light. Similarly, each stage of the password manager adoption is impacted by some positive or negative factors that influence or impede the performance of that stage. If the influential factors are available without the impedance factors, the user can move from one stage to the next. Furthermore, as with nature, the time the process takes to move from stage to another depends on the users and their circumstances. For example, a user who has good levels of awareness about password managers might take less time to plan to use a password manager than a user who has just heard about them. Similarly, a user with high intention to use a password manager may take less time to start searching for one than a user who has a lower level of interest in using this tool. Also, users who have time to search for a suitable password manager can move to the decision stage before those who do not have time.

When someone becomes aware of the existence of these applications, depending on the con-

victions that they have about password managers, they will have an interest in using one to manage their passwords. The user will initiate a search about password managers and the search phase commences. At the end of this phase, users typically end up with a number of applications to choose from. They then enter the decision stage, which incorporates a decision to install one of the applications or to reject the idea. In the case of choosing to install one of these applications, the user moves to the trial phase, where he or she trials the application and decides either to continue using it in the long term or to discard it. At any time in the long-term adoption, when the users are not satisfied with the service provided by the application, they can delete it and search for another password manager to switch to.

3.4.4 Password Manager Adoption Lifecycle

After the three coding steps in Grounded Theory, the final phase in this approach is to conceptualise the categories and the relationships between them in order to develop a theory.

As mentioned in section 3.4.3, the password manager adoption process is similar to the growth process of organisms: it is affected by external factors and requires time to move from stage to stage. The sequence of the developing stages of organisms, like trees, frogs and butterflies, defines their lifecycles. A butterfly lifecycle has four stages. Each stage is different and has a different goal. Also, the lifecycle process can take a month to a year, depending on the type of butterfly. The development stages of a wide variety of insect species are affected by crowding, humidity, host plant species and quality, and light.

Like organism development, password manager adoption has a lifecycle. The lifecycle of password manager adoption is as real as the lifecycle of a frog or a butterfly. Both have sequential phases with start and end points, are affected by external factors and their development time depends on individual conditions. The password manager adoption lifecycle starts after the user becomes aware of and plans to use a password manager. Then, the adoption consists of three stages: search, decide, and try. A successful trial experience leads to long-term adoption.

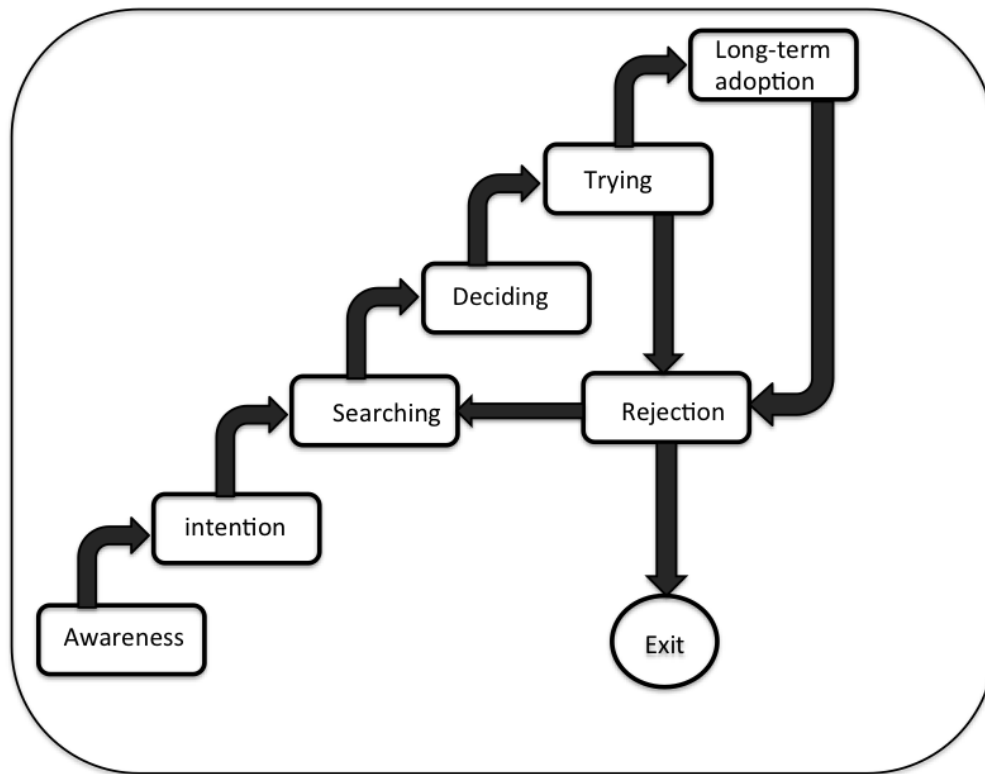


Figure 3.2: Password manager adoption stages

(Source: Developed in this research)

3.5 Adoption Example

This section demonstrates the password manager adoption lifecycle using a fictitious example, showing how the user moves from stage to stage to adopt a password manager.

Alex had many online accounts (emails, social networking accounts, online shopping accounts and an online banking account). She used the same password for all her accounts but she changed the last two letters to incorporate the acronyms of the website name. She was not aware of password managers until she was involved in a discussion with a friend about the recent news that one of the popular web services, Yahoo, had been hacked and the service provider had advised users to change their passwords. Her friend told her that she was not worried because she used a password manager and she used a unique password for each of her accounts. Alex liked the idea of a password manager but she did not have time to search for one and preferred not to spend time searching. Later, the password for her university email expired and she was asked to change it. After few days, she was frustrated because she could not remember what the new password was and she could not access her email. She planned to use a password manager to avoid that from happening again. So, she typed 'password manager' into the App store search

engine and a list of too many password managers was presented. She did not know which one to choose. After a long time comparing them, she decided to install DashLane because it was well rated and she liked the description page. She started using DashLane with her work account, as she had already been asked to reset it with a new password. After a few weeks she liked her experience and decided to move more of her accounts to DashLane.

One day, she wanted to access one of her accounts from her laptop but she could not remember the password and her phone battery had run out. She decided to install DashLane on her laptop and synchronise her passwords on her phone with her laptop, but she found that the synchronisation feature only existed in the premium version of DashLane, which required payment. She did not want to pay for this feature, so, she decided to switch to another password manager that could synchronise between devices for free. She searched again for a password manager, ended up with a number of choices and decided to install LastPass. She moved her passwords from DashLane to LastPass and deleted DashLane.

3.6 Discussion

The adoption stage theory suggests a number of factors that can influence the adoption of password manager applications, which highlights some research gaps. This section discusses recommendations to support the adoption of password managers during the different stages of the application lifecycle.

a. Recommendation for Information Security Advisors:

1. Effective Marketing of Password Managers:

Lack of awareness was a strong reason for the lack of adoption. People will not even embark on the lifecycle depicted in Figure 3.2 if they do not know of the existence of password manager tools. The lack of awareness is puzzling since these applications have been available since 1999 [155]. Due to the sensitivity of password data and the fact that so few people use them, it is unlikely that they are hearing about the apps from friends and family, which may explain the lack of awareness.

There is a clear need for effective marketing if more people are to adopt password managers. The use of word-of-mouth is an important factor to consider. Many adopters in the study reported that they had recommended these tools to friends and family members. In addition to making them aware, knowing about these applications from trusted people increased the trust in password managers and hence their usage. So if a certain critical mass of people start using them and promote them to family and friends, many more will probably follow.

2. Cyber Security Awareness:

Even if people become aware of the apps, they might still not embark on the adoption process. Many people mistakenly think that their current password practice is secure [64]. Some participants believed that they did not need security support tools because they only used one password for all their accounts. Others believed that they were not important and therefore would not be targeted by attackers, or that their data was not valuable so they did not need to worry about their data being hacked. It seems that, in addition to making people aware of these password manager apps, more work is needed in terms of disseminating "good practice" with respect to password behaviour so that people understand that their current behaviour is making them vulnerable to attack. Furthermore, cyber security awareness should be improved by using different awareness strategies for the different internet community members.

3. Support The Adoption Process:

When giving security advice to end users, it is important to make it easy for them to consider the adoption decision from a personal perspective by providing appropriate interventions to facilitate the adoption process. For example, users might be reluctant to apply operating system updates on their smartphones because of their uncertainty about the potential risks of losing particularly personal and sensitive data, such as photos or contact numbers. Providing an accompanying backup option, or explicitly ensuring that no data will be lost during the update request, might improve update installations and encourage people to apply it.

In terms of password managers, the study identified three stages engaged in during password manager adoption. After the users became aware of password managers, and planned to use one, they would commence the process by searching for a suitable one. When the user initiated a search, a number of password managers would be presented, if they decided to proceed, a selection would be made. The time it takes to go through these processes depends on the user's level of awareness of password managers and their existing knowledge. The purpose of the search process could be to reveal any uncertainty, to explore the available features of password managers and to find a password manager with specific features that they expect to find, e.g. open source.

Typically, the search process is conducted by initiating a search in the application store for a 'password manager'. It can also be started by asking other users, as people expect them to be more innovative about password managers and what they would recommend. Furthermore, users can search the web for information about password managers in general. In the decision stage, they need to compare and contrast the different password managers and they usually reason about their own decision. Gathering information, evaluation and the decision making are time consuming and effortful, which might deter users from adopting password managers or at

least impede the process.

Supporting users at this stage with an appropriate intervention could influence the adoption process. For example, the system could recommend a password manager that suits their preferences and needs.

b. Recommendations for Password Manager Developers:

1. Building Trust in Password Managers:

Due to the critical nature of the data manipulated by password managers, users must be able to trust these systems. The study reveals some factors that influence this trust:

Having the source code open and available to everyone to review can increase trust level. Users might not be sure about whether the application has a backdoor to send their passwords to the developers. Also, transparency in reporting hacking incidents increases trustworthiness. Vendors need to explain how it happened and what precautions will be taken to prevent it from happening again.

2. Application Description Page:

This study revealed factors that might deter adoption even if users have heard about the app, and are sufficiently interested in using the tool. A number of the study respondents did not understand how this application worked and was used. It is unfortunate that most of the existing applications in App stores fail to provide this information. Anayle reports that Apple consumers consider the description and the screenshots in App Store Product Pages when they are interested in buying an application [157]. One reviewer suggested the use of video clips to improve the user experience. Yet, many existing password manager applications in Apple and Google Play stores only provide a description of how the application is used. A few provide screenshots of the application interface and they mostly focus on demonstrating the features provided by these tools. They seldom demonstrate how the application can be used. Developers should provide a step-by-step video that shows users how easily they can start using the password manager.

Due to the critical nature of the data manipulated by password managers, users need to be able to trust these systems and they need to know how their passwords are secured and stored, at the very least. So, in addition to demonstrating how to use the application, developers should include simple information about how security and privacy are preserved. Expecting all users to understand technical words, such as AES-256-bit encryption or PBKDF2 technology, is misguided. A simple explanation needs to be added to describe how the data is protected.

3. User Interface:

Some users in the study complained about the password manager interface. Developers should pay attention to designing an interface that ensures easier navigation and requires fewer clicks in order to provide a more intuitive user interface and better user experience.

Other users felt that such a password manager would violate their basic human need for autonomy. Humans need to retain control [158], [149] and password management is no different. It might be that in trying to be helpful by taking away all password-related concerns, these apps make people feel that they have lost the sense of control they need. Password managers might need to work on giving people a sense of control during their operation. This possibly can be achieved by providing as many choices as possible. For example, choices for synchronisation, choices of the cloud third-party service, and choices of the storage location: local on the device or in the cloud. Also, for the cloud, it is possible to provide options for the cloud data centres' locations. Furthermore, it should be made clear in the interface that the system-generated password is optional to use.

The study paid attention to the importance of cross-platform consistency. With the fact that many users might have different devices, designing usable interfaces for each device is not sufficient. Designing for a multi-channel user experience is important for users' satisfaction. Users need a consistent look and feel when they switch from one device to another and password manager applications should be consistent in behaviour and design across different devices and operating systems. However, the study only explored different smartphone OSs. Users might have different expectations and requirements for each device type. For example, they may have different needs when using a password manager from their mobile devices versus a computer in the office. Therefore, investigations into tailored device-specific password manager design and user experience are required.

In addition, the hedonic quality of mobile applications (such as the experience of enjoyment) was mentioned by [159] as an adoption factor. No one in the surveys and reviews spoke about the app being "enjoyable", yet this is clearly something people want. They spoke about being reassured, the reduction of effort, the relief of not having to manage passwords, but no mention was made of enjoyment. Hassenzahl et al. polled 548 people and reported that hedonic quality was strongly associated with the positive experience of an app [160]. This is yet another non-functional quality that app developers could pay attention to, in order to improve adoption.

4. Support Users' Relatedness Psychological Needs:

The study shows the importance of customer support for the users' satisfaction with their expe-

rience of using password managers. This also satisfied the user relatedness basic human need (i.e. feeling connected to others) when using the application and increased confidence in the application, which may positively affect the long-term adoption. Password Manager vendors should create communication channels with their users and keep them active by responding to the users' queries and updating them with the latest news about their application. At the very least, they should respond to the users' reviews in the application store. Also, users would expect to find an email that they can use to send a specific enquires. Furthermore, social networking services, such as Facebook and Twitter, are short-length communication channels and the most used ones. Developers should utilise these services to broadcast their latest news and better serve their users. The feeling of relatedness, or being connected while using the application, can be supported by including icons in the interface that link users to the different communication channels.

3.7 Conclusion

In this chapter, users' perceptions of password managers were investigated. Data were collected from two sources and qualitative analysis was conducted on the basis of the Grounded Theory approach. It has been found that many users were not aware of the existence of password managers. The adoption process goes through stages, starting when the user becomes aware of the existence of these tools. Then, the user searches, decides, installs, rejects or continues using the password manager in the long term. The study reveals some gaps in the adoption literature. To this end, some recommendations have been suggested to developers and security advisors to encourage adoption. The contribution of this work is the identification of the stage theory underlying the adoption of password managers. It reflects the impedances to the widespread adoption of these tools. It identifies the reasons for adopting, or not adopting, password managers. However, it is acknowledged that the study has a limitation in that the reviews authenticity are not validated.

Chapter 4

Theoretical Background

4.1 Introduction

Chapters 1 and 2 have introduced the thesis and contextualised it in relation to the existing literature. Chapter 3 discusses the exploratory study conducted to obtain primary data for the research topic. This chapter presents background information underlying the research approach that has been chosen to derive and substantiate the research findings.

This research focuses on the earlier stages of password management tool adoption with two main objectives: (1) investigating the factors that significantly affect the users' intention to adopt a password manager; and (2) encouraging end users, by means of an intervention, to convert their intention to adopt a password manager into actual adoption.

This chapter reviews the chosen theory used to model the factors that affect the password manager adoption decision. It also discusses the methods/techniques that were chosen to conduct the study into encouraging the adoption of password managers.

4.2 Theoretical Model for Predicting Behaviour Intention

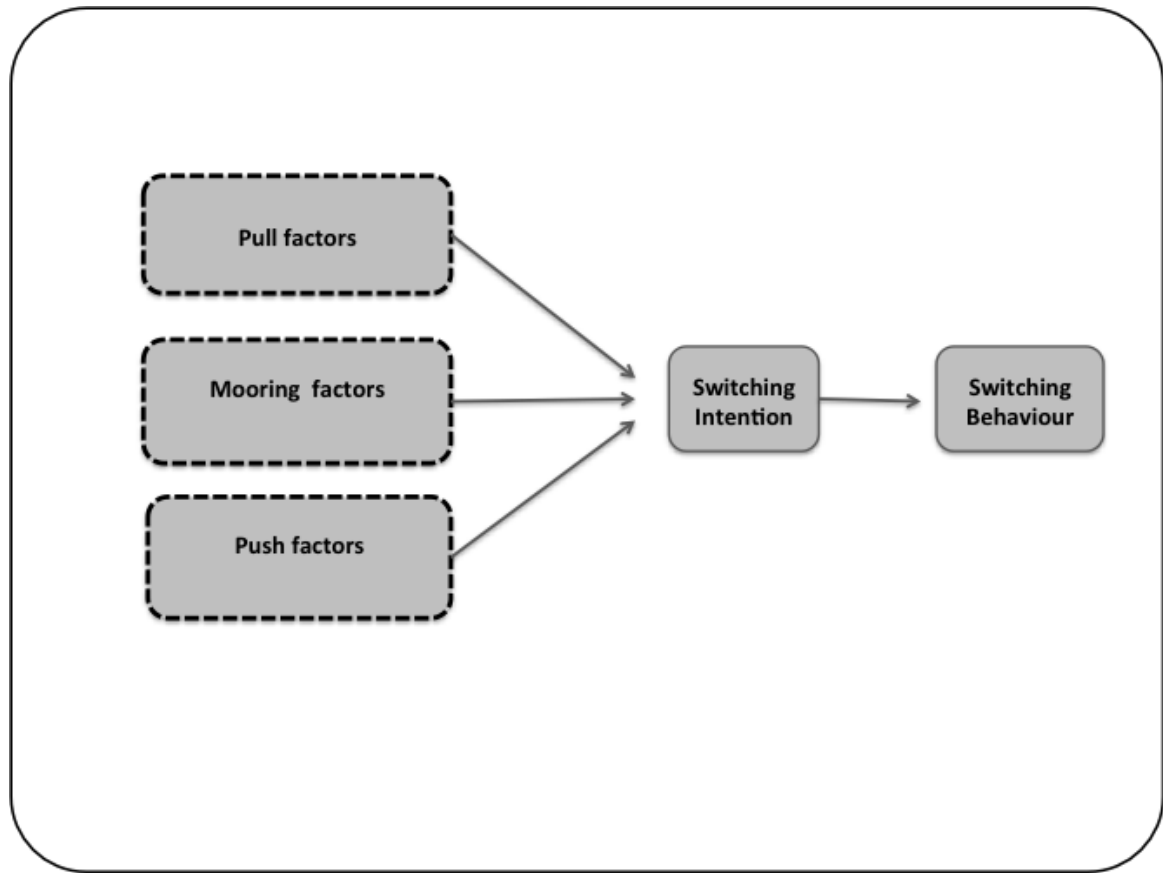
Why the theoretical model is important:

A theory is a set of interrelated concepts, definitions and propositions that systematically explains or predicts events or behaviours by specifying relations between variables [161]. Understanding the information security perspective of users is important as it helps to contextualise users' observed behaviours, as well as to potentially predict their future behaviours [162]. Research and studies on human-centred information security have increased in recent years, following the interest in understanding and influencing users' security behaviours. It has been recognised that human behaviour and perception are the bottleneck for many changes to enhance security [2]. As a result, several behavioural theories and models have been developed and applied to study different information security behaviours. Among these models are: the Health

Belief Model (HBM) [17], Theory of Planned Behaviour (TPB)[165], Social Cognitive Theory (SCT) [166], Theory of Reasoned Action (TRA), Technology Acceptance Model(TAM) [212] and Protection Motivation Theory (PMT) [167]. Applying these theories can guide researchers to understand why users do, or do not, apply the target behaviour, as well as identifying the factors needed to design effective ways to influence and encourage the target behaviour. For example, Van et al. (2013) [18] applied the General Deterrence Theory for designing deterrence-based messages among other different types of messages aiming to influence smartphone user screen lock behaviour. In the same vein, Ngoqo and Flowerday [165] proposed a framework to address the problem of low information security awareness levels among student mobile phone users. They combined TPB with an existing model for measuring information security awareness to understand what triggers student mobile security behaviours. Likewise, a combined model of the protection motivation model and TRA was proposed by Gundu and Flowerday (2012) [167] to examine the factors that influence employee behaviours in small and medium enterprises (SME) towards information security. Then, an e-learning awareness and training program was designed and developed to be used by SME firms in order to promote positive employee information security behaviours.

Switching theory:

Much of the existing research on modelling the adoption of security-related end-user behaviour has relied on the Technology Acceptance Model (TAM) and its extension [192,195,197]. However, this theory involves fixed variables: ease of use, usefulness and behaviour intention. Also, it assumes that adoption is an independent decision. Unlike most of the studied behaviours, in the case of adopting a password manager, the adoption process reflects migration from password coping behaviours to the use of a password manager application. Henceforth, switching theories, such as migration theory, are more likely to reflect actual password manager adoption behaviours. Migration theory describes the reasons for individuals' migration using the concepts of socio-geographical migration theory, i.e. push and pull factors and mooring factors. This theory assumes that migration is the result of negative factors in the current state that encourage people to leave (also called "push factors"); positive factors in the new state that attract people (also called "pull factors"); and the obstacle factors that constrain the migration (also called "mooring factors") (Figure 4.1).



(Source: [170], [171])

Figure 4.1: Migration Theory

Although migration theory originated from geography literature, a number of researchers have investigated switching behaviours in other fields on the basis of this theory. For example, it has been extended to predict migration behaviour regarding the use of cloud computing [169]. Zhang et al. [170] applied the migration framework to explain switching behaviours in online blog services. Also, it has been applied to explain switching between social networking sites [171]. Schreiner et al. [172] applied the theory and examined German-speaking smartphone users' switching intention for mobile instant messaging applications.

4.3 Measuring Actual Information Security Behaviour

Several studies on information security behaviour use a wide variety of research methods for detecting and recording security behaviour. Some studies investigated security behaviour based on self-reported data collected with surveys and questionnaires [125,174,191]. This method can cover a large population given that a questionnaire can be distributed widely and cheaply. However, the reliability of self-reported data is questionable, as self-reported answers do not always reflect actual behaviours. Another method used for studying information-security-related behaviours is lab-based studies [122,176]. However, the synthetic nature of the interaction in lab

experiments makes it hard to reflect the real behaviour of end users. For example, if people are asked to create passwords in a lab experiment, they know the password is unimportant - it will not ever keep them out of a situation where they care about forgetting it. Also, due to the possible social desirability bias that can arise when observing actual security behaviour in a lab, many laboratory experiments in this field are only focused on exploring the usability of a security tool, as well as studying the user's perspective regarding a specific security behaviour. Another method for investigating users' security behaviour is to observe real behaviours [177,162]. For example, Machuletz et al [177] applied the TRA to investigate the determinants that lead notebook users to cover the cameras on their devices (Webcams). They observed the actual covering behaviour of 113 people who used their devices in public places, e.g., libraries, cafes or trains. They also collected self-reported data about their attitudes and subjective norms towards web-cam covering and privacy in general. They found that attitudes towards web-cam covers could predict the actual covering behaviour. Observing actual behaviours is more reliable for reporting security-related behaviours; yet it is difficult to apply to all security-related behaviours. Since the aim of this research requires detecting actual password manager adoption, observation of actual behaviours was used to decide whether users adopted a password manager, or not.

4.4 Recommendation Systems

There are many password manager applications available in the application store. In the Google Play store only, there are over 245 password manager applications. When the user wants to use a password manager app, they need to choose from a vast number of password manager applications that vary in terms of their features and the functions they offer. Evaluating these alternatives to find the best one is time consuming and daunting. Also, a user may choose a password manager app and, when they try it, they may discover that its features are not suitable, leading them to reject the password manager (as found in the exploratory study reported in Chapter 3).

Supporting users in the search for and choosing a password manager is important in order to facilitate their adoption. There are different ways to facilitate the search and decision process. One method is to recommend a particular password manager to the users when advising them to use these tools. However, users may have different personal requirements for the password manager, which might not be offered by the suggested one. Another way to support them is to discuss the requirements with each user then suggesting a suitable password manager. This method can meet the personal requirements of each user, but it is time consuming and it is difficult to reach many people who need to use a password manager. An alternative method is to use an online recommendation system that suggests a suitable password manager based on the users' requirements.

Recommendation systems can support users' decision making in complex information environments for search and selection [178,179]. Also, they improve the effectiveness and efficiency of users' decision making [180,182]. There are different types of recommendation systems, such as collaborative filtering, content-based (profile-based) and knowledge-based recommendation systems [181]. Unlike the other types, knowledge-based recommender systems explicitly use knowledge from users, and knowledge about products to generate recommendations [182]. In some literature, knowledge-based recommender systems are called "search tools" [183]. Blom [184] investigated user experiences when interacting with a recommendation system based on collaborative filtering called "Moviecritic.com". Blom found that users need to understand the algorithm that is used by the system to recommend a particular movie:

“ You need to have some sort of feeling of why it thinks you’re going to like the film, rather than just [have] an arbitrary scale.” [184].

This issue can easily be avoided by using a knowledge-based recommender system. In the case of password manager adoption, users might prefer to specify their personal requirements before choosing a suitable password manager, which can be accomplished by using a knowledge-based recommender system. In addition to giving its users an explicit role in choosing the recommended product, knowledge-based recommender systems are the best choice among the other recommendation systems for critical products that are not purchased very often, such as cars [182] and password managers.

Knowledge-based recommendation systems depend on the following background data: a set of items (in this case password manager applications) I and a set of rules (constraints or features) R that describe each item I . Based on the given user requirements, which are also represented in terms of rules, the system recommends one or more suitable items [185]. This recommender system primarily relies on deep knowledge of the recommended items [185]. So, the first step in designing a recommender system to support password manager choice is to find the different features that describe each password manager and which matter to the user.

Two common pitfalls need to be avoided in designing knowledge-based recommendation systems [183]:

First: The recommendation result itself presents too many items. There are some techniques to mitigate this issue and support user decisions. For example, using critiquing techniques [186] by frequently asking the user to specify their preferences helps to narrow the item space. Another solution is to rank the items and recommend the highly ranked ones [185]. In the case

of the password manager recommender, the items can be ranked based on their ratings in the application store and the apps' popularity (how many times it has been downloaded). The rate and popularity values are already calculated and the values exist in the application store.

Second: The other case is the scenario where no recommendations meet the user's needs. This issue is known in the literature as "Preference Conflict"[183]. Some methods have been developed to deal with this issue based on partial satisfaction techniques. For example, this issue can be avoided by showing the user all the available items that maximally satisfy a subset of their preferences [188]. Another method is to inform the user by presenting other alternative products that are available and partially satisfy their preferences [187]. Alternatively, a browsing-based interaction technique can be used where the user is asked to enter their preferences one at a time and to filter the available items accordingly [183]. This is similar to the critiquing technique in narrowing the item space but in the browsing technique the attributes for choosing preferences also narrow. Since the set of password manager applications is fixed and limited (unlike the typical use of recommendation systems in e-commerce where the availability of items (products) is dynamic), this issue can be addressed by recommending items that maximally satisfy the requirements using a utility function, which ranks the resulting items based on the calculated utility values for each preference.

4.5 Motivational Theories

Encouraging users to engage in secure behaviour is not straightforward. Some researchers suggest that not engaging in security behaviours is related to an incomplete mental model and the underestimation of the risk of their behaviours [86]. Another approach for explaining users' non-adoption of security behaviours is the "compliance budget" [27], [28]. This notion highlights the importance of understanding the cost and benefit of adopting security behaviour, from a users' perspective. It indicates that users make a rational decision to adopt security measures when the benefit of adopting them outweighs the cost of not adopting them. The authors argue that users have a limited budget for complying with security measures and suggest that any effort that adds some cost should be offset with some benefit from the user's perspective [193]. Human motivations have been studied in different research domains [199,200,201] exploring individuals' behaviour and how to encourage the adoption of recommended behaviours. Along these lines, applying motivation theories might positively affect the adoption of password manager security tools.

Motivation theories such as SDT [194] and Pink's motivation theory [158] can offer a theoretical framework for understanding human motivation. Also, the "gamification" approach [196] has a potential effect on motivating humans intrinsically. Human motivation can be classified

into two main classes: extrinsic motivation, which refers to the motivation for the desire to earn rewards such as money; and intrinsic motivation where the person performs an activity for the pleasure and satisfaction derived from the activity itself [15]. Some of the existing studies in the information security domain have focused on the first class [198]. In other research domains, intrinsic motivation has demonstrated a significant impact on users' behaviours [199,200]. In computer science, the role of intrinsic motivation has gained much attention in the game design domain [201].

Self-determination theory (SDT)

According to the SDT, an individual's motivation for performing a certain behaviour, such as adopting a specific tool, can be more or less self-determined. Also, this theory assumes that six types of motivations are associated with any behaviour. These types range from more self-determined motivation such as intrinsic, integrated and identified (also called "autonomous motivations") to less determined motivations, or controlled motivations, such as interjected, external, and amotivation, where the person is not motivated by the target behaviour [202]. Intrinsic motivations are based on the enjoyment and satisfaction that is derived from the behaviour, e.g. using a Pokemon game mobile application. Behaviours that are difficult to describe in terms of enjoyment, such as sharing knowledge on Wikipedia, but that are personally important and align with the person's values, are likely to be representative of "integrated" motivations. Similar to "integrated" motivations, identified motivations occur when the person values the behaviour itself as an important goal. The introjected motivation is based on internalised pressures, such as a feeling of guilt, whereas external motivation refers to a motivation that is stimulated by external factors such as the fear of punishment or the desire for rewards [202].

Schell [201] distinguished between two types of behaviours, namely "wanna" for representing what users want to do and "hafta", which represent what they are obligated to do. Schell stated that the human brain has two different channels: one to seek positive actions and the other to avoid negative ones. He claimed that when people are required to do something without being motivated, their brain records it as a punishment that they need to avoid. This may also explain why users do not adopt security measures that annoy them by clicking "update later" for antivirus update notification messages. Thus, unlike self-determined motivations, controlled motivations are more likely to be presented as "hafta" where the brain records it as a punishment that needs to be avoided. Therefore, this research investigates the effect of applying self-determined motivation on adopting a password manager among smartphone users.

According to the SDT theory, developed by Deci and Ryan in 2000 [194], three basic human psychological needs affect motivation regarding a certain activity: (1) autonomy, (2) compe-

tence, and (3) relatedness. Autonomy refers to the desire to have control over one's own life and to make decision based on one's own choice. Competence is defined as feeling capable of meeting challenges and it involves understanding how to attain efficacious in performing the requisite actions by having enough knowledge to overcome any uncertainty. Relatedness is defined as the need to feel connected to others and to feel like part of something, or to belong to a larger community. This theory has been applied in different sectors to understand human motivations such as Education [204], Health Care [205], and Video Games [163]. For example, it has been used in education to investigate the effect of intrinsic motivation on teachers' intention to use or not to use digital learning materials [204]. It has been also applied in the health sector to understand smokers' basic psychological needs and hence design intervention programmes to encourage smoking cessation [205].

Applications of SDT for human behaviours:

Wohn [164] found that the need for fulfilment of autonomy, relatedness, and competence are significant predictors of self-determined motivation for playing online games based on self-reported survey on 1011 mechanical Turk users. Gagne [168] argue that self-determined motivation can moderate the link between the intention to share knowledge with others and the actual behaviour. Thus, more autonomous motivation (in contrast to controlled motivation) should strengthen this link.

Wiklund et al. [173] explored the sources of fulfilment for six basic human needs, developed by Sheldon [13], when using interactive products and media. They carried out a study on ten participants using an open-ended questionnaire. They found that the flexibility in using the product at anytime, anywhere, as well as the freedom of choosing whatever product one prefers, are the two main sources for supporting autonomous feelings. Furthermore, the competence basic need was implied by Usability, Novelty, Mastery and Knowledge. They also found that communication with others, information in terms of news, sharing with others and the brand name can fulfil relatedness basic needs. Szalma [175] claimed that interfaces that are high in motivational usability, through their use, could satisfy the user's needs for autonomy, competence, and relatedness. Furthermore, he stated that autonomy could be supported by an interface or task that provides the user with as many choices as possible and is practical in terms of setting immediate and long-term goals. They also found that the lack of choices might thwart autonomy satisfaction.

Rayan et al. [163] conducted a user study on gaming to find the relationship between games that satisfy autonomy, competence, and relatedness needs, and players' intrinsic motivation. They compared Mario 64, which affords relatively limited choices over actions and environ-

ments, with more elaborate multiplayer online games. They found that the online game players were more willing to play again in the future. Silva et al. [189] showed four different strategies that can be used to support autonomy:

- Choice: by encouraging users to follow their own interests and providing options whenever possible,
- Relevance: by providing clear and meaningful reasons why a particular activity is advantageous, facilitating self-endorsement,
- Respect: by acknowledging the importance of users' perspectives, feelings and agendas and
- Avoidance of control: by not using coercive, authoritarian, or guilt-inducing language or methods.

They claimed that competency can be supported by:

- Clarity of expectations: by explaining and discussing what to expect and not expect from the behaviour-linked outcomes,
- Optimal challenge: by tailoring strategies and goals to the individual skills,
- Feedback: by offering clear and relevant informational feedback and
- Provision of instrumental and practical skills training, guidance, and support.

Staunton et al. (2015) [190] applied SDT in a computer-based intervention to deliver persuasive messages that promoted dental flossing. They designed the messages based on SDT to increase the control feeling and intrinsic motivation. To increase perceived control, they used phrase like "when you successfully made changes in health practices and achieve things well" and "describing how you managed to make this change and how it felt to succeed", rather than the phrases "when you felt unable to stick to the changes in health practices you set out to achieve" and "focusing on the difficulties that prevented you from successfully making these changes". Furthermore, they used phrases like "in line with your values and the things that are important for you" to increase intrinsic motivation compared to the phrase "the main reason for them to want you to use dental floss regularly". In a 2*2 factorial experiment, they found that this intervention had a strong effect on self-reported flossing behaviour a week after the intervention. Sweeney et al. [12] examined an application of SDT and word of mouth (WOM) within online communities aiming to enhance energy-saving behaviours. They designed and developed an online intervention in the form of a community website that supported autonomy, competence and relatedness needs. They claimed that the autonomy needs were supported in two ways: first, participation

was voluntary. Second, continued engagement would suggest that users considered the website and its content to be of personal interest and/or importance. They claimed that users would have seen their competence increase, as they were exposed to expert information, followed by the opportunity to reflect on this content by discussing it with their peers. Also, users were invited to participate in competitions and challenges to test their knowledge and practice, as well as to see how they fared against their peers. They also declared that the participants' feeling of relatedness was supported as the website created an online community around the topic of energy saving, giving its users the opportunity to vote in polls, take part in competitions and challenges, and discuss energy saving with others, which means that they became part of a community and interacted with other users. The intervention was tested in a controlled experiment that included an experimental group with users who had access to the website as well as a control group that did not know about the website. They found a significant increase in the self-reported energy-saving behaviours over time, supporting the role of SDT. Also, they found that positive WOM increases satisfaction of the three psychological needs of autonomy, competence, and relatedness, and influences energy-saving behaviour.

Fathali et al, [14] investigated the effect of the three motivation determinants (autonomy, competency and relatedness) on learning English among Japanese students. Using a web-based e-portfolio system, they tested the learners' intention to continue learning the language beyond the classroom as well as their actual performance. The system was designed to support learners' autonomy, competency and relatedness by including a page with a link to an online test; a page with a list of different learning websites for their users to choose from; a page for instructors to give weekly feedback, which assisted the learners and referred them to other online material; a page for learners to self-assist and set future learning goals; and a page that grouped all the learners' individual web pages to enable them to receive feedback from the instructors and their peers on the weekly assignments. On this page, each learner could upload a weekly file of their reading practice, which included their learning activities, such as writing summaries and making questions. The learners had access to all of the members' e-portfolios and could post comments. Also, they were randomly assigned to pairs to ensure everyone would receive a weekly comment. Using self-reported questionnaires, the authors found that perceived competence had the strongest effect on the learners' intention to continue learning the language outside of the classroom and on their actual learning achievements. Likewise, the results reflected a strong relationship between perceived autonomy and the learners' intention and actual behaviours. However, they did not find evidence that relatedness could influence the learners' achievement. They attributed that to different reasons. First, the design of the system emphasised the sense of connectedness but also supported the individuality of the learners by having personal e-portfolio that allowed the learners to identify their own learning progress with their own distinct learning styles in their own e-portfolios. Second, the majority of the learners were

at the same level of English language proficiency, which means they could not acquire or master their knowledge with the help of each other and hence their relatedness cannot be an influential factor for their actual achievements. The third reason is related to the Japanese students' cultural beliefs and educational system, which rely on teacher-centred learning environments, meaning that peer-supported learning is not highly valued by these students.

To sum up, SDT has been applied successfully in many different domains in different contexts to reason about individuals' motivations and to encourage the adoption of certain behaviours. It is therefore a promising approach in the context of information security to encourage the adoption of password managers.

4.6 Conclusion

This chapter provides descriptions of the theories grounding this research. First, the selection of migration theory for this research is justified. Second, the justification of the choice of a knowledge-based recommendation system is presented. Finally, SDT was introduced and related studies were presented to demonstrate its potential in the domain of interest. The next chapters use the described theories and techniques to answer the research questions by building and testing a theoretical model for predicting the adoption of password managers and designing and testing an intervention to encourage the adoption of this tool.

Chapter 5

Adopting Password Manager: A Migration Theoretic Analysis

5.1 Introduction

This chapter presents and empirically validates a theoretical model of smartphone users' adoption of a password manager. The main factors, extracted from the initial exploratory interviews with 30 smartphone users, were used to build a framework of password manager adoption using Migration theory as a theoretical base. The proposed model of password manager adoption was validated in a longitudinal study with smartphone users. This study contributes to the growing body of knowledge on information security behaviour by drawing attention to password manager adoption as a promising solution to the password problem, expounding the main factors that influence or hinder password manager migration, and introducing Migration theory as a reference theory to the information security literature.

5.2 Theoretical Model

Since password managers deal with sensitive data, they have more sensitive features than other security tools and users might have different perspectives in terms of adopting them. An exploratory study was conducted to gain insight into users' perceptions of such a system, and hence to identify the best theoretical framework with which to model the password manager adoption process (section 5.3).

The qualitative data reveals that password manager adoption decisions are affected by perceptions related to the password manager itself and perceptions related to the user's current password coping mechanisms.

Most of the existing models and theories for technology adoption and behaviour change assume that adoption is an independent decision. These theories might be suitable for studying independent behaviours where the new adopted behaviour does not substitute an existing one. For

password managers, the adoption process reflects a switch from password coping behaviours to the use of a password manager application.

Table 5.1: Security behaviour studies

Previous Studies	Security Behaviour	Influencing Factors		
		Related to the current state	Related to the recommended behaviour	Other factors
Ngoqo and Flowerday (2015),[165]	Mobile security behaviours		Attitudes (+), Perceived behavioural control (+)	Subjective norms (+)
Vafaei-Zadeh (2018) [217]	Adopting internet security software		Relative advantage (+), Compatibility (+), Ease of use (+), Visibility (+), Result demonstrability (+), Triability (+)	Voluntariness (+) image (+)
Machuletz (2016) [177]	Webcam covering behaviour	Attitudes (+)		Subjective norms (+)
Djeni, I. and Erbilek (2017) [220]	Adopting biometric system		Privacy concerns (-), Perceived security (+), System quality (+), Performance expectancy (+)	Innovativeness (+)

Reviewing selected recent research into security behaviours in the field of information security (Table 5.1) shows three key categories of predictors influencing the studied behaviour. First, users' adoption or intention to adopt a secure behaviour is affected by their perception of their current behaviour, such as the perceived severity or vulnerability of an online threat. Second, users' behaviour or behavioural intention is affected by their perception and expectations of the targeted behaviour, which can either positively influence the adoption (such as response efficacy) or negatively hinder it (such as response cost or privacy concerns). Third, individual differences such as a user's innovativeness can predict adoption behaviours. Innovativeness is the degree to which the user is relatively early in adopting new technologies compared to other users in their community.

Finding a theory that can integrate all of these predictors in an inclusive framework is beneficial. It can help guide switching behaviour research, gives rational guidance with respect to the choice of latent factors and hypotheses in potential information security switching behaviour studies, and assists in interpreting their findings and results.

Unlike other theories in the information system domain involving fixed factors, such as ease of use, usefulness and behaviour intention in the Technology Acceptance Model, and the certainty

and severity of sanctions, and behaviour compliance in the General Deterrence Theory, the Migration theory does not mandate fixed variables of the pull, push, or mooring factors. Migration theory, from the human geography literature, forms a comprehensive framework that can represent switching behaviours [19]. This theory assumes that migration is the result of negative factors in the current state, which encourage people to leave (also called 'push factors'), positive factors in the new state that attract people (also called 'pull factors'), and the obstacle factors that constrain the migration (also called 'mooring factors').

Because the context of the migration behaviour plays a role in pinning down the influential factors, this theory does not specify the exact pull, push or mooring factors. Instead, it draws the general framework for the migration phenomenon. Lee (1966) [19] stated that migration behaviour is more influenced by migrants' perceptions of the pull, push and mooring factors than the real objective effects of these factors.

A number of researchers have investigated switching behaviour in the information system field on the basis of migration theory. It has been extended to penetrate switching behaviour to the use of cloud computing [169], instant messaging services [215] and social network services [216]. Unlike other applied theories in information security fields, Migration theory considers factors related to the current behaviour as well as the new recommended one, providing a wider view of the users' behaviour. Also, this theory assumes that behaviours are different from each other and that each is affected by its own influential factors; thus the factors in this theory are not pre-defined.

In this chapter, Migration theory is used as a theoretical lens to explain users' migration to password management applications.

5.3 Eliciting Study (Semi-structured Interview)

Most technology adoption studies build their theoretical models by picking and choosing variables from a list of factors that have been empirically tested in other information technology adoption studies. Since password managers are different from other technologies and because of the limited literature on password manager adoption, interviews were used as the initial data collection method for constructing the adoption model. Semi-structured interviews were conducted in order to generate discussions that made it possible to obtain insight into users' thoughts instead of posing direct questions with a 'yes' or 'no' response, which might frame users' responses and not provide extra information. Fishbein and Ajzen [221] advised conducting a survey using open-ended questions with the target population to gain further understanding of the desired behaviour. They suggested that a sample of 30 participants from the target population is sufficient to gain an exhaustive insight into adopting the target behaviour and extract the salient beliefs about this behavior [221]. Therefore, semi-structured interviews were conducted from April to June 2016 with 30 smartphone users. The questionnaire can be found in Appendix

B, and the study was approved by the University of Glasgow ethics board. Participants were recruited using social networking and they were informed that a 50p donation would be paid to support Cancer Research for each participant, up to a maximum of £50. Upon completion of the study, a copy of the receipt from the Cancer Research Centre was posted on the researcher's own web page so that the participants could see that the donation had been made. The sample consisted of participants with different education levels, with an average age of 36.3 years. Of these, 18 were females (60%), and 12 were males (40%). The majority were Android users.

The transcripts of the interviews were analysed using thematic analysis, focusing on identifying themes and patterns related to perceptions about password managers and the features the participants liked about password managers or wished to find in these tools. First, three interviews were coded and then they were coded again, independently, by a second coder. After that, a joint codebook was created, which was used to code all the interviews. As each new idea or perception was encountered, it was discussed with the second coder to agree on a new code before it was added to the codebook (Table 5.2).

Table 5.2: Factors affecting users' decision to adopt a password manager

No	Factor affecting the adoption	Example	Frequency (%)
1	Relative Usefulness	"...I cannot remember what asks for what because some of them want a capital letter they want an @symbol they want a monkey you know you've no idea what they want so I cannot remember what rules apply to what website so it's a great advantage cos I can just whip it and do it and it means if I'm on an unfamiliar computer I've got all my passwords on my phone so I can just have a quick look and go ..."P2	29 (96)
2	Perceived Risk in general	"I don't trust these services. just trust myself more than I trust an external service basically"P25	26(86)
3	Concern about Security Risk	"what is the security level of this password manager because so many people they they decode all these softwares and they hack these softwares. So,security level is another concern"P13	23(76)
4	Descriptive Norm	"maybe if um my friends were using it and were telling about it"P11	19(63)
5	Password Managing Cost, (Dissatisfaction)	"it is difficult to remember them all because it keeps telling you to change them for security things sometimes you just can't remember what they are you know", P26	14(46)

Table 5.2 continued from previous page

No	Factor affecting the adoption	Example	Frequency (%)
6	Response Efficacy	"...makes them more secure against attack"P4	13(43)
7	Concern about Privacy Risk	"so if you heard about something quite hot issue in the previous 2 or 3 weeks is about the FBI in America they would like to access [um] the mobile phone the [the] iPhone. They asked apple to [encrypt] to de decrypt [uh how to say] data in the mobile"P9	10(33)
8	Perceived Vulnerability (Dissatisfaction)	"Sometimes I don't feel secure. Like when I am in public I try not to open my account as I don't know if someone is watching through a CCTV camera for instance" P3	9(30)
9	Learning Cost	"...especially the old people they quite unfamiliar with the IT with the new technology so normally they need time to learn how to use it", P10	9(30)
10	Set-up Cost	"if I have time then maybe I'll configure it [I guess] to use it"P12	7(23)
11	Financial Cost	"if it was free..." P17	6(20)
12	Innovativeness	"I wouldn't tend to take the initiative to em be the first one to try something"P18	5(16)
13	Perceived Ease of Use	"I am assuming an easy app..something that is just simple quick to use ..." P27	5(16)
14	Concern about Access Risk	"if you forget your password or the system goes down your snookered you cannot get in to anything can you!" P19	5(16)
15	Phone Device Related Problem	"My phone is quite an old. So there is no space..."P30	5(16)
16	Decision Support	"I am thinking about starting to use one but not sure if I know which password manager is the best" P3	4(13)
17	No Need (No Dissatisfaction)	" I remember all of my own passwords and I've got [em] different security that offers [like] from microsoft so that would eliminate the need for a password manager occasion" P20	4(13)
18	Subjective Norm	"if I am working with other people and using the same drop[...] share a folder in dropBox and so maybe it is important that everyone has a strong password and so in that case someone could be interested in me having a software that manage passwords" P30	3(10)
19	Lack of Information	"you know ..if people can understand it they can start use it like its more about creating awareness about it demonstrating the use of it and highlighting its importance...." P13	3(10)

Table 5.2 continued from previous page

No	Factor affecting the adoption	Example	Frequency (%)
20	Concern about Efficiency	"if the password manager is slow. low fetch passwords and decrypt them.. You know.. maybe I will feel it is, delaying me instead of saving my time" P3	2(6)

As mentioned in section 5.2, the extracted factors can be categorised into factors related to password managers, factors related to the current password behaviour and other factors affecting the adoption of a password manager. Those related to password managers support the adoption (positive) or deter the adoption of this tool (negative). This suggests that the adoption decision depends on a combination of factors that provide reasons to change current password management methods, factors that represent reasons to move to the password manager and factors that represent the obstacles or difficulties that hinder the adoption of a password manager. Therefore, Migration theory seems to be the most appropriate theory to model the password manager adoption process.

Table 5.3: Push, Pull and Moor factors

Pull Factors	Push Factors	Mooring Factors	Other Factors
Relative Usefulness (+), Response Efficacy (+), Perceived Ease of Use(+).	Password Managing Cost (Dissatisfaction) (+), Perceived Vulnerability (Dissatisfaction)(+), No Need (No Dissatisfaction)(-).	Perceived Risk in general(-), Concern about Security Risk(-), Concern about Privacy Risk(-), Learning Cost(-), Set-up Cost(-), Financial Cost(-), Concern about Access Risk(-), Phone device Related Problem(-), Concern about Efficiency(-).	Descriptive Norm (+), Innovativeness (+), Decision Support (+), Subjective Norm (+), Lack of Information(-).

5.4 Password manager Migration Model

Since many factors emerged from the interviews, only the significant ones will be included in the model. Fishbein and Ajzen [221] suggested that people's beliefs about a particular behaviour can be identified by checking the frequency of each theme in the collected qualitative responses then selecting themes identified by at least 20% of the answers (i.e. if they were mentioned by at least 6 interviewees)[221]. Therefore, the following factors were chosen in the model:

5.4.1 Pull Factors

Pull factors are password-manager-related factors that attract users. Two main pull factors emerged from the analysis of the interviews as attractive reasons to use password managers: (1) the usefulness of password managers compared to not using one and (2) their effectiveness in improving the security of the user's passwords and online accounts. This confirms previous research on the adoption of security tools and measures. A study showed that perceived effectiveness of security policies had a positive influence on individuals' intention to comply with these policies [222]. Furthermore, according to the IT adoption literature, one of the strongest predictors of adopting new technology is the user's perception of how useful that adoption will be, i.e. 'perceived usefulness'. Instead of evaluating the perceived usefulness independently, in the case of technology migrations, usefulness is evaluated against the user's current state before adopting the new technology. In the literature, this construct is called 'relative usefulness' [169]. Therefore, two hypotheses are proposed:

Hypothesis 1: *Perceived relative usefulness of password managers is positively related to the users' intention to adopt this tool.*

Hypothesis 2: *Perceived response efficacy of password managers is positively related to the users' intention to adopt this tool.*

5.4.2 Push Factors

These are the factors that push users away from their current password coping behaviours towards the use of password managers. Prior research shows that a primary reason for users to adopt new technology is their dissatisfaction with their current product or service [169], [223]. Dissatisfaction is the state of being unhappy about a service or a product based on poor experience. If the users' evaluation of their current method for managing their passwords is unsatisfactory, they are more likely to migrate to the use of a password manager, compared to those users who are satisfied with their current password management methods. Based on the analysis of the interviews, the main sources of this dissatisfaction are: (1) the perceived cost of managing

passwords and (2) perceived vulnerability. Because the severity of these factors depends on the number of passwords the user has, and their hacking experience, they have been included as control variables.

Hypothesis 3: A user's dissatisfaction with their current password coping method is positively related to their intention to adopt a password manager.

Hypothesis 3.a: The perceived vulnerability of a user's current password coping method is positively related to their dissatisfaction with their existing method.

Hypothesis 3.b: The perceived cost of managing passwords with the current password coping method is positively related to the users' dissatisfaction with this method.

5.4.3 Mooring Factors

Despite the presence of pull and push factors related to password manager adoption, some factors might intervene with the migration if they exist. Previous migration-theory-based research found switching cost to negatively affect migration intention [169], [172], [216]. Likewise, the results of the interviews revealed that the costs associated with password manager migration - such as set-up cost, learning cost and monetary cost - discourage the adoption of this tool. Furthermore, given the sensitivity of data stored in a password manager, and due to the potential risk when using these tools, users might be reluctant to adopt them. Therefore, the perceived risk of password managers is included as a mooring factor. Security and privacy concerns over using password manager applications were found to be the main factors influencing the perceived risk of using these tools.

Hypothesis 4: The perceived risk of using password managers is inversely related to the users' intention to adopt this tool.

Hypothesis 4.a: Security concerns over using a password manager tool are positively related to the users' perceived risk of using this tool.

Hypothesis 4.b: Privacy concerns about using a password manager are positively related to the users' perceived risk of using this tool.

Hypothesis 5: The perceived cost of learning how to use a password manager is inversely related to the users' intention to adopt this tool.

Hypothesis 6: The perceived cost of setting up a password manager is inversely related to the

users' intention to adopt this tool.

Hypothesis 7: *The perceived monetary cost of using a password manager is inversely related to the users' intention to adopt this tool.*

5.4.4 Other Factors

Besides push, pull or mooring factors, there are other factors that impact on the decisions of switching to the password manager, such as descriptive norms.

Descriptive Norms

Descriptive norms, also called social influence in the literature, are defined as "what individuals perceive others around them are commonly doing" [225]. It has been found to be a predictor for the intention to adopt security systems [226], [227] such as anti-virus software [227]. Also, the analysis of the interviews revealed that users were reluctant to adopt password managers because they "do not want to be first" among their friends and family members to do so. Therefore, this factor has been added to the model.

Hypothesis 8: *The descriptive norms of using a password manager are positively related to the intention to adopt this tool.*

5.4.5 Intention and Actual Adoption

While the intention to adopt a password manager reflects the likelihood of adopting a password manager, actual adoption behaviour is whether users actually install a password manager on their devices or not. The extant human behaviour literature identifies behaviour intention as a main antecedent of actual behaviour [221]. It has been proven to have a significant bearing on actual behaviour [254], [228]. Due to difficulties in recording actual security behaviours, many studies on information security stop short of studying them [229]. Instead, they measure security intention and argue that it is a reasonable proxy for actual behaviour [229]. A systematic review of information security policy compliance studies found that few studies investigated actual behaviours [230]. The study concluded that the best predictor of actual security behaviour is the behaviour intention [230]. Thus, this hypothesis is proposed:

Hypothesis 9: *The intention to adopt a password manager is positively related to the actual adoption of this tool.*

5.5 Methodology

5.5.1 Study Design

The hypothesised model of password manager adoption was tested empirically using a longitudinal survey with Android Smartphone owners. Smartphone users were reasonable subjects for the study because people increasingly rely on their mobile devices to access their online accounts. An online survey was developed to measure the model components using scales derived from the literature. As the majority of smartphone owners own Android devices [231], and in order to measure the impact of the migration model factors including actual behaviour, a mobile application named CyberPal was developed as an Android application. The application was used as a mobile-based platform for harnessing the survey. CyberPal also detected the installed/uninstalled applications on users' devices. The purpose of using the application as a vehicle for the survey was to allow the researches to explore the impact of the migration model factors and also detect actual adoption behaviour. More details about the application is provided in Chapter 6.

5.5.2 Measurement

The measurement items come from extant literature and were modified slightly to fit the study context (Table 5.4). Because the smartphone is the most popular device for accessing the Internet, it was chosen to target the research population.

Table 5.4: Measurement item descriptions

Construct	Definition	Measurement items	No. Of items	Ref
Pull Factors				
Relative Usefulness	The degree to which users believe that adopting a password manager will improve their task performance compared to the other method for managing passwords	(1) Using a Password Manager will help me accomplish my tasks more quickly than my current method for managing my passwords. (2) Using a Password Manager will improve my performance as compared to my current method for managing my passwords. (3) Using a Password Manager will enhance my effectiveness more than my current method for managing my passwords. (4) I will find using a Password Manager to be more useful than my current method for managing my passwords.	4	[169]

Table 5.4 continued from previous page

Construct	Definition	Measurement items	No. Of items	Ref
Perceived Response Efficacy	Users' belief that using password manager will be effective in improving passwords' security and hence reducing the risk of online accounts being compromised or hacked.	(1) Password manager application works for protecting my passwords from being stolen and abused by attackers. (2) Password manager application is effective solution for protecting my passwords from being stolen and abused by attackers. (3) When using a password manager application, my passwords are more likely to be protected from being stolen and abused by attackers.	3	[232]
Mooring Factors				
Perceived Risk	The degree to which users believe that if they use a password manager, they will suffer from potential problems such as losing passwords.	(1) Providing password manager with my passwords would involve many unexpected problems. (2) It would be risky to put my passwords in a password manager. (3) There would be high potential for loss in saving my passwords in a password manager.	3	[233]
Security Concern	Users' concerns about the security level of password manager applications	(1) Password managers implement security measures to protect my passwords from being hacked (R). (2) Password managers usually ensure that transferring information is protected from hacking attacks (R). (3) I feel safe in saving my passwords on password managers (R). (4) I feel secure in managing my passwords using password managers (R).	4	[234]
Privacy Concern	Users' concerns about the probability of having passwords and personal information disclosed as a result of using a password manager	(1) Using a password manager leads to a loss of control over the privacy of my passwords and personal data. (2) Using a password manager allows others to view my passwords and personal data. (3) Overall I see a privacy threat linked to password manager's usage.	3	[235]

Table 5.4 continued from previous page

Construct	Definition	Measurement items	No. Of items	Ref
Set-up cost	The perceived effort and time required to set up the password manager and start using it	(1) It will take a lot of time to set up my device and online accounts to use a Password Manager. (2) It will take a lot of effort to set up my device and online accounts to use a Password Manager. (3) Overall, the process involved in setting up a Password Manager is very elaborate.	3	[169]
Learning cost	The perceived effort and time needed to learn how to use a password manager and get used to it	(1) It will take me a lot of time to learn to use a Password Manager's features. (2) It will take me a lot of effort to get up to speed and use a Password Manager. (3) Learning to use a Password Manager well will be difficult.	3	[169]
Perceived fee	The monetary costs of using a password manager.	(1) The fee that I have to pay for the use of a password manager would be too high. (2) The fee that I have to pay for the use of a password manager would be reasonable (R). (3) I would be pleased with the fee that I have to pay for the use of a password manager (R).	3	[236]
Push Factors				
Dissatisfaction	The degree to which users are dissatisfied with their current way for managing their passwords	How do you feel about your overall experience with the current method for managing your passwords? (1) Extremely dissatisfied... Extremely satisfied. (2) Extremely unpleasant... Extremely pleasant. (3) Extremely terrible... Extremely delightful.	3	[169]

Table 5.4 continued from previous page

Construct	Definition	Measurement items	No. Of items	Ref
Perceived vulnerability	The degree to which a user believes that they are likely to experience cyber attack.	(1) There is a chance that someone could successfully guess at least one of my passwords. (2) There is a chance that someone could successfully crack at least one of my passwords using password cracking software. (3) There is a chance that someone could hack into at least one of my important email accounts. (4) If someone hacked into my important email account there is a chance that they could guess my other important passwords	4	[237]
Response cost of managing passwords	User perception about the cost of managing passwords without password manager.	(1) Managing my passwords currently requires a considerable investment in Time. (2) Currently, there are too many overheads associated with Managing my passwords. (3) Managing my passwords currently requires a considerable effort other than time. (4) Managing my passwords currently causes problems such as memorability issues and task delay.	4	[238]
Other Factors				
Exposure to hacking	Prior exposure to a hacking incident experienced by either the user or someone they know personally and the degree to which the experience affected them.	(1) Have you ever had an important email account a social networking account an online shopping account or online banking account hacked? (Yes, No). Please indicate the degree to which that experience affected you (in terms of lost data, lost time, monetary losses, identity theft etc.) (2) Has someone you know personally ever had their important email account, social network account, online shopping account or online banking account, hacked into? (Yes, No). Please indicate the degree to which that experience affected you (in terms of lost, data, lost time, monetary losses, identity theft etc.)	2	[237]

Table 5.4 continued from previous page

Construct	Definition	Measurement items	No. Of items	Ref
Innovativeness	The degree to which the user is relatively early in adopting new technologies than other users in their community	(1) Other people come to you for advice on new technologies. (2) In general, you are among the first in your circle of friends to acquire new technology when it appears. (3) You can usually figure out new high-tech products and services without help from others.	3	[239]
Descriptive Norm	Users' perceptions about whether others in their social or personal networks are using password manager or not.	(1) Most of my friends are using a Password Manager. (2) Most of my family members are using a Password Manager. (3) Most of my co-workers are using a Password Manager. (4) Most people I know are using a Password Manager.	4	[240]
Intention	The extent to which the user would like to use a password manager in the near future	(1) I intend to use a password manager within a week. (2) I predict I will use a password manager within a week. (3) I plan to use a password manager within a week.	3	[232]
Adoption behaviour	The actual adoption of a password manager	Regularly retrieving all the applications installed in the users' phone device and checking for an installed password manager application	-	-

* R is the reverse item.

Exposure to hacking and perceived vulnerability relied on two- and four-item measures, respectively, adapted from [237]. For response cost for managing passwords, four items were adopted from [238]. Both the intention and the perceived response efficacy measures relied on three items each, adapted from [232]. Users' dissatisfaction, learning and set-up costs were all measured with three items adapted from [169]. Also, four items were used from the same source to measure relative usefulness. Regarding the perceived risk, three items were used from [233]. The perceived privacy concerns and security concerns were measured with three items adapted

from [235] and with four items proposed by [234] respectively. The four items used to measure the descriptive norm came from [240]; the three items used to assess users' 'innovativeness' were adapted from [239]. All of these items used seven-point Likert scales, mostly ranging from 'strongly disagree' (1) to 'strongly agree' (7). Finally, the dependent variable actual behaviours were measured by periodically retrieving all the applications installed in the users' smartphones and checking whether or not they had installed a password manager.

The questionnaire was reviewed by two security and information management researchers, who confirmed its validity. Before initiating the large-scale survey, a pilot test of the questionnaire was also conducted with a convenience sample of 15 users from various education levels.

5.5.3 Data Collection

An invitation to participate was sent to 219,221 Android users, using the Facebook advertising service, between July and September 2017. Users were asked to install the application, answer the questionnaire and keep the application on their devices for a week for the chance to win online vouchers up to £50. 645 users responded to the invitation and participated in the study. In order to obtain valid data, only users who were aware of password managers were included in the study. Thus, users were asked whether they were aware of password managers or not. Further, they were asked to select the names of two popular password managers from amongst five names of mobile applications. The five application names actually contained only two password managers. The rest were names of screen-locking mobile applications. Among the received responses, only 232 participants reported that they knew about password managers. After reviewing the responses, 12 did not complete the questionnaire, 7 did not answer the validation question correctly, 1 did not keep the application for a week and 14 did not engage with the survey. After discarding these responses, 198 completed and usable responses were retained for analysis.

5.6 Data Analysis and Results

The data analysis proceeded in four stages:

- The first stage screened the data to ensure validity to support subsequent analysis;
- the second stage involved a descriptive analysis of the dataset;
- the third stage focused on assessing the validity of the construct used in the model and
- the last stage was directed at hypotheses testing and model analysis using Structural Equation Modelling (SEM).

The data was analyzed using SPSS 23 and AMOS 23 software.

5.6.1 Data Screening

Before commencing the analysis, the data were screened to evaluate their validity and to see if they met the assumptions of Structural Equation Modeling (SEM). Therefore, several tests were conducted using SPSS23. First, the data were scanned for missing data. From the scanning process, 6 cases were identified with missing data that were randomly distributed. Using SPSS, the Missing Completely at Random (MCAR) test confirmed that these missing values were indeed completely random ($p = .785$). Little's MCAR test is a mechanism used to examine the randomness of the missing data. Missing data are MCAR when the probability of missing data on a variable is unrelated to any other measured variable and is unrelated to the variable with missing values itself [241]. The MCAR value indicated that missing values in the dataset were randomly missed ($p > .05$). These missing data were imputed using the median value technique, a technique that is commonly applied to compensate for missing values in quantitative studies. Data normality is considered an important assumption for further statistical analysis. Non-normality of the data is indicated when the data are either highly skewed or when there is kurtosis, which renders some statistical tests inaccurate and produces random effects in the results. Kurtosis is the extent to which the peak of a unimodal probability distribution deviates from the shape of a normal distribution ; whereas Skewness is the measure of the lack of symmetry (asymmetry) of the probability distribution. If the skewness value is greater than 2, then the data are positively (right) skewed, while if it is less than -2 they are negatively (left) skewed [242]. Likewise, if the absolute overall kurtosis score is 2 or less, then there is no kurtosis [242]. The non-normality is more often interpreted by the existence of outlier cases in the dataset. An outlier is a case in the collected data with an extreme value on one variable. The descriptive analysis of the dependent and independent variables was conducted in SPSS (Table 5.5). This table shows that the kurtosis values for all the variables are less than 2 and the skewness scores are all within the acceptable range, which suggests that the data are normally distributed. The outliers were tested by evaluating the standardised Z scores of (± 3.29) in each variable [243](p.107). The standardised Z values for the dataset were between valid ranges. This process was followed by evaluating linearity and homoscedasticity, which are important assumptions for linear regression models [244]. Linearity is the existence of a linear relationship between the dependent and independent variables in the model [244]. Homoscedasticity is defined as the presumption that the variance of errors is the same across all levels of the independent variable. It describes the case where the variance of the dependent variables is the same across all the levels of the independent data [244]. Linearity and homoscedasticity were evaluated by examining the scatter plots in SPSS [245]. The inspection of the scatter plots revealed an oval shaped array of points, suggesting that variables are linearly related and homogenously distributed.

Table 5.5: Descriptive statistics

Construct	Min	Max	Mean	Std. Deviation	Skewness	Kurtosis
Exposure to Hacking (HACK)	.00	6.50	1.1667	1.78189	1.607	1.734
Security Concerns (PWMSEC)	1.00	6.75	4.4874	1.38124	-.411	-.782
Perceived Risk (PRISK)	1.00	7.00	4.8283	1.51016	-.189	-1.272
Privacy Concerns (PWMPRIV)	1.33	7.00	4.9226	1.17966	-.186	-.577
Intention (INT)	3.00	7.00	5.0606	1.25386	.005	-1.235
Monetary Cost (PWMFEE)	1.33	6.67	4.6633	1.21050	-.819	.191
Set-up Cost (PWMSETC)	1.67	7.00	4.6330	1.55115	-.033	-1.432
Learning Cost (PWMLC)	1.00	6.67	3.9764	1.26362	.017	-.752
Response Cost of Managing Passwords (RCMAN)	1.25	7.00	4.7828	1.09402	-.146	-.310
Relative Usefulness (RU)	1.25	7.00	4.6073	1.16262	-.086	-.343
PM Response Efficacy (PWMREFF)	2.67	7.00	5.0488	1.08592	-.104	-1.104
Innovativeness (INNOV)	1.67	7.00	4.7744	1.28054	-.219	-.802
Descriptive Norm (DNORM)	1.00	6.00	2.0909	1.52536	1.157	-.088
Dissatisfaction (DISSAT)	1.33	6.67	4.1380	1.00311	.062	-.287
Perceived Vulnerability (PVUL)	2.25	6.50	4.7247	.96742	-.170	-.537

Finally, to examine whether two or more constructs represent the same construct, a multicollinearity test is required [244], [243]. Multicollinearity can be detected in the data when two different variables share a high correlation (≥ 0.90) [243]. Table 5.6 shows that inter-correlations between variables range from .06 to .83. Also, multicollinearity can be evaluated through the Variance Inflation Factor (VIF)[245]. If $VIF > 10$ then this is an indication that two variables are highly correlated and a multicollinearity problem is presented [245]. Using SPSS, calculated VIF values ranged from 1.201 to 5.011 (Table 5.7), which did not exceed the recommended cut-off value of 10. This means the correlations between predictors are not high and there is no multicollinearity among factors.

Accordingly, this stage ensured that the data set of size 198 was valid and usable for testing the hypotheses.

Table 5.6: Correlation Matrixes

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

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

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

Table 5.7: Variance inflation factor

Construct	Collinearity Statistics	
	Tolerance	VIF
Exposure to Hacking	.735	1.361
Set-up Cost	.283	3.536
Learning Cost	.353	2.833
Security Concerns	.474	2.108
Perceived Risk	.200	5.011
Privacy Concerns	.437	2.290
Monetary Cost	.750	1.334
PM Response Efficacy	.413	2.420
Innovativeness	.489	2.043
Descriptive Norm	.461	2.167
Dissatisfaction	.482	2.076
Perceived Vulnerability	.832	1.201
Response Cost of Managing Passwords	.663	1.508
Relative Usefulness	.410	2.437

a. Dependent Variable: Zscore(INT)

5.6.2 Descriptive Analysis

During this phase, a descriptive analysis of participants' demographic data was conducted. Table 5.8 shows the demographic profiles of the respondents and their password manager app usage. Most respondents (70%) were under the age of 35; 64% of these were male and 36% were female. In terms of their education, 24% of the participants reported that they had a Bachelor's degree and 23% held a higher education degree, whereas 9% claimed that the highest level of school they had achieved was less than a high school diploma. Only 3 participants were already using a password manager app on their Android devices.

Table 5.8: Descriptive Data

Gender	Frequency (%)	PM usage	Frequency (%)
Male	128 (65)	Already using a PM	3 (1)
Female	68 (34)	Not using a PM	195(98)
NA	2(1)		
Age	Frequency (%)	Education	Frequency (%)
		Less than a high school diploma	18(9)
18-25	87 (44)	High school degree or equivalent	32 (16)
26-35	53 (27)	Some college, no degree	40 (20)
36-45	37 (19)	Associate degree	12(6)
46-55	16 (8)	Bachelor's degree	48(24)
56+	4 (2)	Master's degree	30(15)
NA	1 (.5)	Professional	9 (5)
		Doctorate	7(4)
		Other	2(1)

5.6.3 Measurement Model

A measurement Model represents the relationship between the variables and their measures [244]. This stage aims to examine the model by assessing both the constructs' validity and reliability and the model-fit indices, which are used to estimate the measurement model. A Confirmatory Factor Analysis (CFA) was conducted to achieve this aim using both AMOS and SPSS.

Construct validity and reliability:

In the CFA model, items are grouped according to the component definition from which the items came. Then, the item groupings are combined to form composite scores. If the composites show satisfactory measurement properties, they can be used in the final structural model [244], [245].

The CFA is conducted to evaluate the degree to which a set of indicators constructing a scale all measure one thing in common [245]. This uni-dimensionality can be evaluated by testing both the convergent and discriminant validity of all the constructs in the model [246].

Convergent validity is the extent to which the measures that are theoretically related are correlated [246]. Evaluating convergent validity relies on three indicators: the item reliability of each construct, the reliability of each construct; and the Average Variance Extracted (AVE) for every construct [243], [247].

First, convergent validity is assessed by examining the loading of each indicator, in the measurement model, on their constructs. Items should only be retained if they have a strong factor loading, which indicates that the construct is well defined by its items [244]. It has been recommended to retain the items in the measurement model that have a factor loading exceeding 0.50 [244]. The factor loading of each item was computed in the CFA analysis using the AMOS tool. As shown in Table 5.9, the loading of all items is greater than the cut-off value of 0.50 with all critical ratios (t-value) above 1.96, indicating that all the items are strongly related to their relevant factors. The critical ratio (C.R.) is formed by dividing an estimate (factor loading) by its standard error.

Table 5.9: Standardized Regression Weights

Construct	Item no.	C.R (t-value)	Factor Loading
Intention	1	*	.902
	2	21.137	.919
	3	20.005	.900
Perceived Vulnerability	4	*	.849
	3	14.644	.848
	2	14.753	.852
	1	14.670	.849
Monetary Cost	3	*	.923
	2	20.902	.928
	1	17.274	.845
Innovativeness	3	*	.923
	2	20.757	.906
	1	21.094	.911
Privacy Concerns	3	*	.849
	2	16.827	.912
	1	16.179	.888
Security Concerns	1	*	.817
	2	13.910	.851
	3	13.723	.842
	4	13.709	.842
Set-up Cost	1	*	.930
	2	23.039	.919
	3	24.367	.934
Dissatisfaction	1	*	.866
	2	16.993	.901
	3	16.423	.881

Table 5.9 continued from previous page

Construct	Item no.	C.R (t-value)	Factor Loading
PM Response Efficacy	1	*	.899
	2	19.372	.917
	3	16.148	.836
Response Cost of Managing Passwords	1	*	.857
	2	16.337	.887
	3	15.576	.862
	4	15.068	.845
Relative Usefulness	1	*	.867
	2	14.733	.824
	3	14.748	.824
	4	16.536	.880
Learning Cost	1	*	.850
	2	13.638	.815
	3	14.079	.833
Descriptive Norm	1	*	.914
	2	24.548	.944
	3	26.251	.962
	4	27.837	.976
Perceived Risk	1	*	.933
	2	25.797	.942
	3	26.328	.947
Exposure to Hacking	2	*	.828
	1	6.585	.655

Another indicator for verifying the convergence between the items and the factors is the average percentage of variance AVE, extracted from a group of the items of each construct. AVE is computed for each construct by adding all the squared values of the factor loading of its items and then dividing the sum by the number of items representing the construct [244]. The value of AVE should be at least 0.5 for it to be acceptable, indicating that a factor explains more than 50% of the variance of its items [244]. The AVE was calculated using the Stats Tools Package developed by Gaskin [248]. Table 5.10, presents the AVE output for all constructs. The table reveals that the AVE values for all constructs are greater than the minimum accepted point (0.50). Therefore, it is concluded that all the items converged into their respective factors.

Table 5.10: Average variance extracted for validity testing

Construct	AVE (>0.5)
Perceived Risk	0.885
Intention	0.823
Perceived Vulnerability	0.722
Monetary Cost	0.809
Innovativeness	0.834
Privacy Concerns	0.780
Security Concerns	0.702
Set-up Cost	0.861
Dissatisfaction	0.779
PM Response Efficacy	0.783
Response Cost of Managing Passwords	0.745
Relative Usefulness	0.721
Learning Cost	0.694
Descriptive Norm	0.901
Exposure to Hacking	0.557

Convergent validity can also be evaluated through construct reliability. Construct reliability is the degree to which a set of two or more indicators (items) share the measurement of that construct. It measures the internal consistency and homogeneity of the items that comprise each scale [244]. A construct is highly reliable when all its items are highly correlated, indicating that they are measuring the same construct. Construct reliability can be tested with Cronbach's Alpha. Cronbach's Alpha is a statistic commonly quoted by authors to demonstrate that tests and scales that have been constructed or adopted for the research are fit for purpose. A Cronbach's Alpha value of 0.70 or higher suggests good construct reliability [244]. It has been also suggested that an alpha value between .60 and .70 is acceptable [244]. Construct reliability was computed using SPSS. Table 5.11 shows the Cronbach's Alpha values for all variables. All the reliability scores in the study ranged between .703 and .973, supporting the convergent validity of the measurement model.

Table 5.11: Constructs' Reliability

Construct	Number of items	Cronbach's Alpha
Perceived Risk	3	.958
Intention	3	.933
Perceived Vulnerability	4	.910
Monetary Cost	3	.926
Innovativeness	3	.937
Privacy Concerns	3	.914
Security Concerns	4	.904
Set-up Cost	3	.949
Dissatisfaction	3	.913
PM Response Efficacy	3	.914
Response Cost of Managing Passwords	4	.921
Relative Usefulness	4	.910
Learning Cost	3	.871
Descriptive Norm	4	.973
Exposure to Hacking	2	.703

Discriminant validity is the degree to which concepts that should not be related theoretically are not inter-correlated [246]. It can be verified when the correlation value shared between a construct and any other construct is less than the correlation value of the construct and its items [244]. Therefore, if the square root of the AVE value of a construct is greater than any correlation between this construct and any other construct, then that construct is more correlated with its indicators than any other construct in the model. A correlation matrix is a table showing correlation coefficients between variables. Each cell in the table shows the correlation between two variables. The correlation matrix for discriminant validity was generated by the Stats Tools Package developed by Gaskin [248] using output from CFA analysis in AMOS. As shown in Table 5.12, the square root of AVE values, represented in the top of each column (range from 0.747 to 0.949), is greater than any other correlation in that column. This indicated that all constructs in the model are different from each other, supporting the discriminant validity of the model scales.

Table 5.12: Discriminant validity

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

*Values in bold represent the square root of AVE in Table 5.10

Model Fit:

The next stage in evaluating the measurement model is to measure the model fit in order to determine the extent to which the indicators (items) operationalise the latent variables (constructs). The measurement model fit refers to how well the proposed model of the factor structure reasons about the correlations between variables in the dataset [244], [249]. If the model is able to account for all the main correlations in the model, then the model has a good fit. If not, then there is inconsistency between the correlations proposed and the correlations observed in the data, and the model is low fitted. A low-fitted model requires changes and modifications in the original model to enhance the fit [245], [250]. There are different statistics used to determine the goodness of model fit. Commonly used measures are: Chi-square, Comparative Fit Index (CFI), the Incremental Fit Index (IFI), the Turker-Lewis Index (TLI) and the Root Mean Square Error of Approximation (REMSEA) [243], [244]. Table 5.13 shows the minimum accepted cut-off points for all these measures.

Table 5.13: Model Fit Indices cut-off values

Acceptance level	Model Fit		Model Comparison		
	χ^2/df	RMSEA	IFI	TLI	CFI
Acceptable scale for good adequate fit	≤ 2	$<.06^{**}$	$\geq .90$	$\geq .90$	$\geq .90$
Recommended for further analysis	> 2	$>.08$	$<.90$	$<.90$	$<.90$

* Source ([249],[250]) ** (Reasonable fit up to .08)

The measures for the model fit were computed through CFA analysis in AMOS. The goodness of fit values for the measurement model are specified in Table 5.14. These values are all within the acceptable scale for a good fit specified in Table 5.13, indicating that the measurement model fits with the sample data.

Table 5.14: Summary of overall measurement model

Fit Indices	Overall Measurement Model
χ^2/df	1.136
RMSEA	.026
IFI	.985
TLI	.983
CFI	.985

5.6.4 Structural Model

Using Structural Equation Modelling SEM for data analysis has become popular recently in the information management literature. Generally, a SEM model is composed of two sub-models: (1) a measurement model and (2) a structural model [245]. The measurement model defines the relationships between the observed and latent variables. The structural model, however, explains the relationships between the latent variables in order to test whether a particular latent variable influences another latent variable in the proposed theoretical model [244], [245].

This section reports the result of testing the hypotheses proposed in Section 5.4 Using the AMOS 23 tool, the hypotheses were tested through structural equation modelling using the model in Figure 5.1 as a base model.

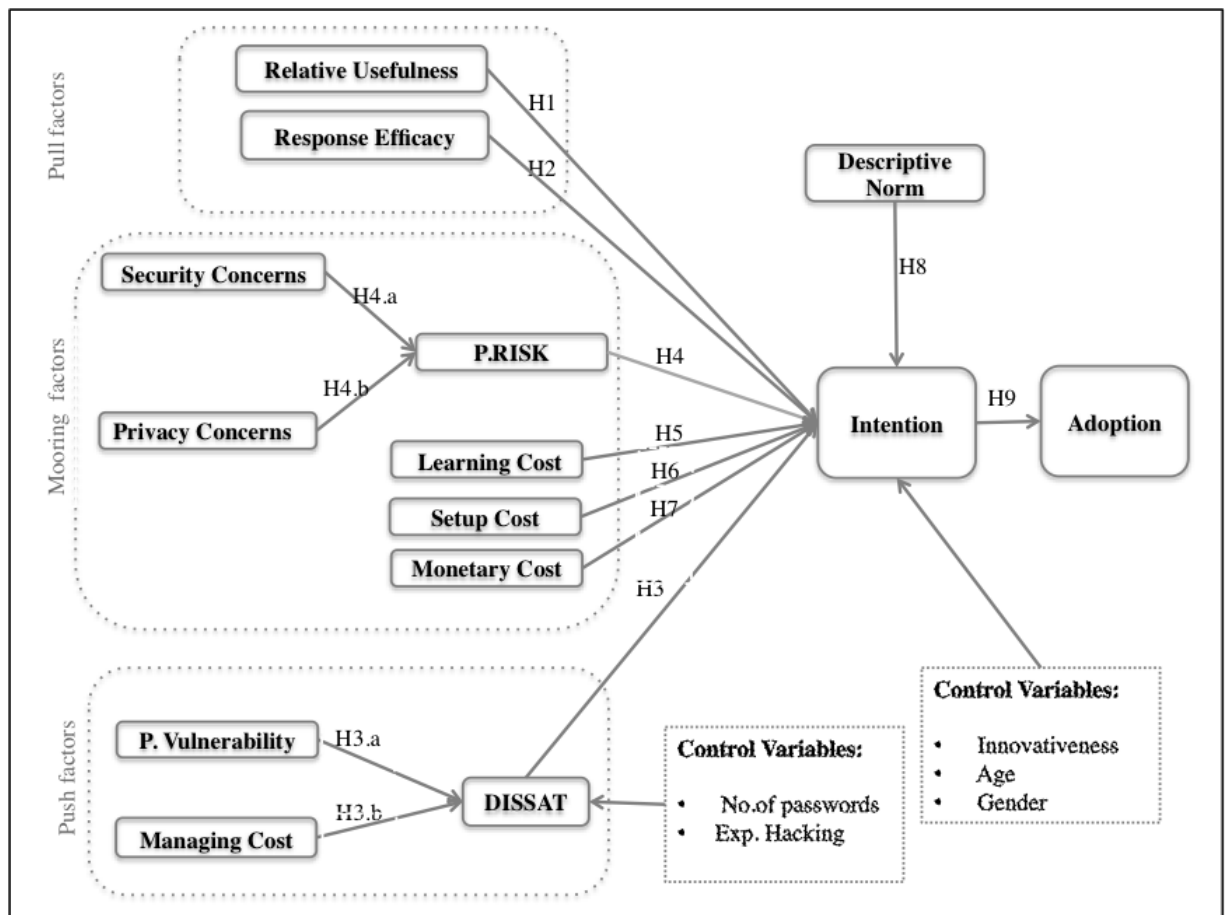


Figure 5.1: The proposed conceptual model with hypothesis

Different techniques are used to explain the structural model. In order to assess the goodness of fit of the proposed relationships between the constructs to the data, several model-fit indices were evaluated. These included normed chi-square ratio, CFI, IFI, TLI and RMSEA. Furthermore, as suggested [244],[245], the parameter estimates of the structural model were examined to understand the effect of the independent variables on the dependent variables, as suggested in the theoretical model.

As illustrated in Table 5.15 , the normal chi-square value was 1.557, indicating a good fit of the structural model. Also, the RMSEA value was .053, which implies adequate model fit. . Further, IFI= .990, TLI= .948, CFI= .989 suggesting a reasonable fit of the model to the data. To sum up, the evaluated values of the fit indices indicated that the proposed structural model fitted the dataset well. The regression weight for each variable loading into its relevant latent variable was between 0.655 and 0.976, with critical ratios (t-value) greater than the minimum cut-off value 1.96, which indicates that the relationships between each latent variable and its factors are statistically significant(Table 5.9).

Table 5.15: Structural equation model results

Variables	Intention	Adoption	Risk	Dissatisfaction
Independent Variables				
Intention		.626*** (9.343)		
Descriptive Norm	.105** (2.727)			
Relative Usefulness	.178*** (4.321)			
PM Response Efficacy	.140*** (3.355)			
Monetary Cost	.010 (.314)			
Set-up Cost	-.373*** (-7.515)			
Learning Cost	-.021 (-.463)			
Perceived Risk	-.182*** (-3.584)			
Dissatisfaction	.076* (2.077)			
Privacy Concerns			.371*** (6.030)	
Security Concerns			.981*** (9.567)	
Perceived Vulnerability				.202*** (3.193)
Response Cost of Managing Passwords				.229*** (3.492)
Control Variables				
Innovativeness	.082* (2.192)			
Age	.021 (.733)			
Gender	-.027 (-.941)			
Exposure to Hacking				.261*** (4.096)
Number of Passwords				.075 (1.219)
Model Fit				
X ² /df= 1.557, IFI= .990, TLI= .948, CFI= .989, RMSEA= .053				

(***p<.001, **p<.005, *p<.05)

Hypothesis Testing:

As highlighted before, the SEM approach encompasses two steps: the measurement model evaluation using CFA, and the structural model. The structural model can be tested to examine the hypothesised relationships between the constructs in the theoretical model [245]. This section aims to test the relationships between the latent variables in the password manager adoption model. As depicted in Figure 5.1, the model has a number of hypotheses focusing on the main construct "intention", and four more hypotheses centering on the "perceived risk" and "dissatisfaction" constructs. The SEM output reported in Table 5.15 was evaluated based on the path coefficient value, critical ratio CR (t-value) and p-value. The standard measures used to evaluate the significance of the relationships between the independent and dependent variables are CR value of at least 1.96, and p-value less than or equal cut-off point .05 [250]. The following sections report the results of testing these hypotheses.

Pull Factors:

As reported in section 5.4, two hypotheses were developed regarding the pull factors (hypotheses one and two):

H1 Perceived relative usefulness of password managers positively related to the user's intention to adopt this tool.

H2 Perceived response efficacy of password managers positively related to the user's intention to adopt this tool.

Perceived relative usefulness and intention

As illustrated in Table 5.15, the path coefficient from relative usefulness to intention in the hypothesised model was significant (path coefficient= .178 with critical ratio=4.321 and p-value less than or equal to .001), which supports hypothesis one. This finding is in line with prior research that studied the influence of users' perceived usefulness of critical services on their intention to adopt them [169], [251], [252]. Thus, the more the users believed that using a password manager would be useful, the greater the intention to adopt it.

Therefore, it can be concluded that users' perception of the relative usefulness of password managers, compared to not using them, is of high importance for their intention to adopt a password manager.

Perceived response efficacy and intention

Hypothesis two predicted a positive relationship between perceived response efficacy and intention. Table 5.15 indicates that perceived response efficacy positively affects intention ($\beta = .140$ with t-value=3.355 and p-value $\leq .001$), which supports hypothesis two. Therefore, the results confirm the strong relationship between users' perception of the effectiveness of password managers (in improving the security of their accounts and passwords) and their intention to adopt a password manager. This finding is consistent with prior studies that found a strong relationship between users' perceived response efficacy and their intention to enable security measures on their devices [226], [238].

Push Factors:

In section 5.4, the theoretical model proposed a relationship between users' dissatisfaction with their current method for managing their passwords and their intention to switch to a password manager. This dissatisfaction is influenced by users' perceived vulnerability and the response cost for managing their passwords. Thus, three hypotheses were developed:

H3 A user's dissatisfaction with their current password coping method is positively related to their intention to adopt a password manager.

H3.a The perceived vulnerability of a user's current password coping method is positively related to their dissatisfaction with their existing method.

H3.b The perceived cost of managing passwords with the current password coping method is positively related to the users' dissatisfaction with this method.

Dissatisfaction and intention

Table 5.15 shows a positive relationship between dissatisfaction and intention (path coefficient value of .076 with t-value = 2.077 and p-value less than .05), in support of hypothesis three. Previous scholars proved that people's dissatisfaction influences their intention to switch their behaviours [169],[223]. Therefore, users' dissatisfaction with their current coping methods for managing their passwords influences their intention to switch to password managers.

Perceived vulnerability and dissatisfaction

The model predicted a positive relationship between perceived vulnerability and dissatisfaction. The SEM results in Table 5.15 support the prediction ($\beta = .202$ with t-value = 3.193 and p-value $\leq .001$). Thus, users' dissatisfaction with their current password coping method is strongly related to their perception of being vulnerable to cyberattacks.

Response cost of managing passwords and dissatisfaction

The estimated path coefficient value of the relationship between the response cost of managing passwords and dissatisfaction is relatively high (= .229) and significant (t-value = 3.492 and p-value $\leq .001$). This supports the proposed hypothesis that the response cost related to managing passwords without a password manager has a positive effect on users' dissatisfaction with their current password management coping behaviour.

Mooring Factors:

The theoretical model developed in section 5.4 suggested four factors affecting intention negatively: perceived risk, learning cost, set-up cost and monetary cost. The perceived risk, in turn, is predicted by privacy and security concerns. Therefore, six hypotheses were developed:

H4 The perceived risk of using password managers is inversely related to the users' intention to adopt this tool.

H4.a Security concerns over using a password manager tool are positively related to the users' perceived risk of using this tool

H4.b Privacy concerns about using a password manager are positively related to the users' perceived risk of using this tool.

H5 The perceived cost of learning how to use a password manager is inversely related to the users' intention to adopt this tool.

H6 The perceived cost of setting up a password manager is inversely related to the users' intention to adopt this tool.

H7 The perceived monetary cost of using a password manager is inversely related to the users' intention to adopt this tool.

Perceived risk and intention

The path coefficient from perceived risk to intention in the proposed model was significant (path coefficient= -.182 with critical ratio= -3.584 and $p\text{-value} \leq .001$), which supports hypothesis four. This finding is consistent with the findings that perceived risk strongly impacts users' intention to use online services [253], [254], [255]. Accordingly, users' perception of the risk of using a password manager deters their intention to adopt it.

Security concerns and perceived risk

Security concerns are predicted to be a strong factor influencing perceived risk. This prediction is supported by the results in Table 5.15. The standardised estimated path coefficient for the relationship between the two constructs is high (.981) and significant ($p\text{-value} \leq .001$ and $t\text{-value}=9.567$). Other research also supports this finding [256] [224]. Hence, users' security concerns when using a password manager strongly influence their risk perception related to this tool.

Privacy concerns and perceived risk

Privacy concerns are another factor predicting perceived risk. The result of analysing the structural model reveals that the path coefficient for the relationship between privacy concerns and perceived risk is significantly high ($\beta = .371$, $t\text{-value}=6.030$ and $p\text{-value} \leq .001$). Previous studies proved the relationship between the two variables [233],[253]. This implies that the privacy concerns of using a password manager positively affect users' perception of the risk of using a password manager.

Learning cost and intention

In section 5.4, learning cost was identified as a mooring factor. To test the effect of learning cost on users' intention to adopt a password manager, Table 5.15 shows the path coefficient of the relationship between the two variables is -.021 with t-value= -.463 and p-value >.05. This result indicates that there is no evidence from the data that learning cost influences intention to adopt a password manager. Consequently, hypothesis five is not supported.

Set-up cost and intention

Another suggested factor deterring the intention to adopt a password manager is the cost associated with setting up a password manager. SEM analysis illustrated that the relationship between set-up cost and intention is significant ($\beta = -.373$ with t-value= -7.515 and p-value $\leq .001$). Therefore, the perceived cost of setting up a password manager negatively affected the intention to adopt this tool.

Monetary cost and intention

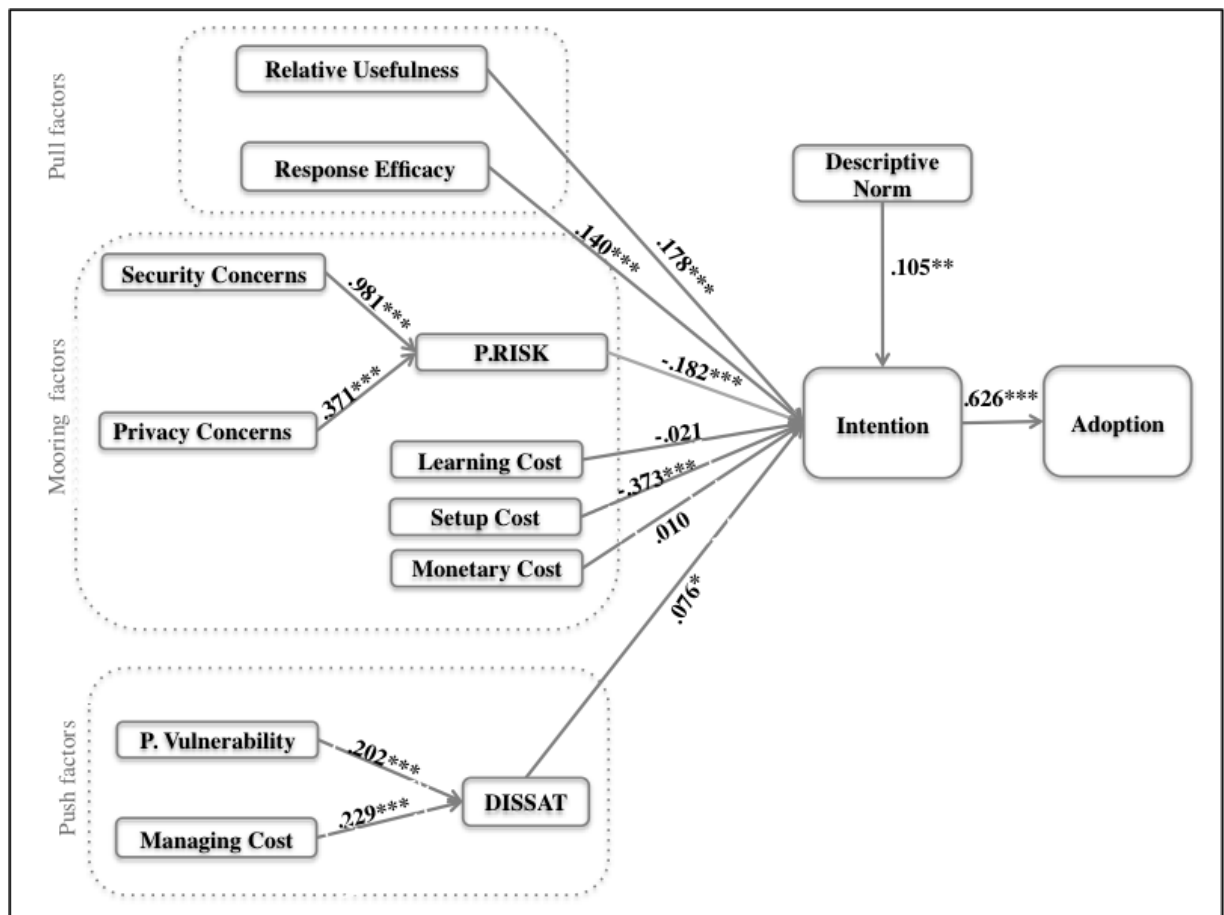
The last mooring factor proposed in the theoretical model is the financial cost linked to the use of a password manager. Table 5.15 shows that the relationship between monetary cost and intention is not significant ($\beta = -.010$ with t-value= .314 and p-value > .05), which does not support hypothesis seven.

Descriptive Norm and Intention:

Another factor proposed to influence the intention to use a password manager is the descriptive norm (social influence). The path coefficient of the relationship between the descriptive norm and intention is .105 with t-value= 2.727 and p-value $\leq .005$. This indicates that the descriptive norm significantly influences the intention to adopt a password manager, hence hypothesis eight is supported.

Intention and Adoption Behaviour:

The theoretical model in section 5.4 suggested that the actual adoption of a password manager is predicted by the intention. Table 5.15 shows that the standardised estimated path coefficient value of the relationship between the two variables is high ($\beta = .626$) and significant (p-value $\leq .001$ and t-value= 9.343). This finding is in line with much existing research on human behaviour. Therefore, the actual adoption of a password manager is predicted by a prior intention to adopt this tool; consequently, hypothesis nine is supported.



(*P < .05, **P < .01, ***P < .001)

Figure 5.2: Hypothesis testing results

Summary of Hypotheses:

Table 5.16 presents the results of testing the hypotheses. It can be noted that six out of the eight links between the intention variable and its independent variables were found to be statistically significant. The effects of learning and monetary costs on intention were not statistically significant. Additionally, intention significantly predicts the actual adoption. Furthermore, all the relationships between the dependent variables perceived risk and dissatisfaction and their independent variables were statistically significant.

Table 5.16: Hypothesis testing results

	Hypothesis	Result
H1	<i>Perceived relative usefulness of password managers is positively related to the users' intention to adopt this tool.</i>	Accepted
H2	<i>Perceived response efficacy of password managers is positively related to the users' intention to adopt this tool.</i>	Accepted
H3	<i>A user's dissatisfaction with their current password coping method is positively related to their intention to adopt a password manager.</i>	Accepted
H3.a	<i>The perceived vulnerability of a user's current password coping method is positively related to their dissatisfaction with their existing method.</i>	Accepted
H3.b	<i>The perceived cost of managing passwords with the current password coping method is positively related to the users' dissatisfaction with this method.</i>	Accepted
H4	<i>The perceived risk of using password managers is inversely related to the users' intention to adopt this tool.</i>	Accepted
H4.a	<i>Security concerns over using a password manager tool are positively related to the users' perceived risk of using this tool.</i>	Accepted
H4.b	<i>Privacy concerns about using a password manager are positively related to the users' perceived risk of using this tool.</i>	Accepted
H5	<i>The perceived cost of learning how to use a password manager is inversely related to the users' intention to adopt this tool.</i>	Rejected*
H6	<i>The perceived cost of setting up a password manager is inversely related to the users' intention to adopt this tool.</i>	Accepted
H7	<i>The perceived monetary cost of using a password manager is inversely related to the users' intention to adopt this tool.</i>	Rejected*
H8	<i>The descriptive norms of using a password manager are positively related to the intention to adopt this tool.</i>	Accepted
H9	<i>The intention to adopt a password manager is positively related to the actual adoption of this tool.</i>	Accepted

5.7 Discussion

This section aims to discuss the findings reported in section 5.6 in order to reveal the antecedents of adopting password manager applications. The study identified eight factors directly affecting the intention to adopt a password manager, namely: descriptive norm, relative usefulness, response efficacy, perceived risk, monetary cost, learning cost, set-up cost and dissatisfaction. However, the quantitative analysis shows that only six factors are significant. The factors that influence perceived risk, according to the study, are security and privacy concerns, while dissat-

isfaction is influenced by perceived vulnerability and the response cost of managing passwords. In addition, intention predicts the actual adoption of a password manager.

A growing number of studies in the information security literature provide evidence that the descriptive norm (social influence) influences the intention to perform information security-related behaviours [169],[219]. Furthermore, the descriptive norm was found to be an important factor affecting the intention to adopt an innovation technology [210],[213]. This study supports that argument, and suggests that the perception of password managers being popular and widely adopted influences the intention to adopt a password manager. Therefore, if a critical mass of users start using password managers, many more users will probably follow them.

The use of a password manager supports human memory to retrieve a password for a given account, and eliminates the need to use fallback authentication. Therefore, it saves users' time and allows them to accomplish their tasks with less effort. Additionally, the auto-fill feature of password managers eliminates the effort of typing a long and complex password, and avoids typing errors and switching between keyboard keys, especially on a small smartphone screen. Users' perceptions of the advantages of a password manager in improving their task performance, compared to not using it, predict their intention to use it. This is consistent with prior research. Bhattacharjee [169] found that relative usefulness could predict users' intention to use cloud-based services. Similarly, it has been revealed that the relative usefulness of social networking services (SNS), as compared to blogs, influenced bloggers' switching intention to SNS [252]. It is important to emphasise the advantages of using a password manager in improving the users' overall task performance, as compared to not using it, in order to foster their intention to use it.

Furthermore, users' perception about the efficacy of password managers in protecting their passwords and online accounts influences their intention to adopt a password manager. The role of perceived response efficacy in strengthening intention is found in many studies in different contexts. The effectiveness of SNS as an expression function of the account owners strengthens the willingness of bloggers to switch from traditional blogs to the use of SNS [252]. As password managers are not only a utility tool, but also act as a security measure, the effectiveness of this tool is particularly important to behavioural intention. In addition, prior studies on information security have consistently suggested that perceived effectiveness could predict the motivation to perform security behaviours [209].

Regarding the push factors to switch to a password manager, users' dissatisfaction with the way they are currently managing their passwords predicts their intention to adopt a password manager. Evidence of the influence of dissatisfaction on strengthening intention to switch to disruptive technology exists in the literature [169],[223]. The study reveals that users' dissatisfaction with managing their passwords is mainly due to the cost of managing passwords. Having

many passwords for different accounts required spending time to identify the correct password for each account, or led the user to use fallback authentication and reset their password each time. Even if the user records these passwords in a notebook, carrying this notebook everywhere and reviewing it each time they want to access an account is arduous and time consuming. Another source of dissatisfaction is users' perception of being vulnerable to cyberattacks. As a means to cope with the cost of managing many passwords, users tend to use memorable passwords or reuse the same password across many accounts. This method, in turn, might affect users' perception of the security level of their passwords and online accounts, consequently influencing their dissatisfaction with their current method of managing passwords.

Password manager switching is negatively affected by other factors. Users' perceptions of the cost of setting up a password manager for the first time were found to be a strong deterrent factor. The set-up process includes sign-up and accounts moving. As mentioned earlier, users already have their own coping methods for managing their passwords. Having many passwords for different accounts makes it a tedious and time-consuming process to move each of these accounts with their passwords to the password manager. Furthermore, the perceived cost of setting up a password manager may be influenced by the perception that the process of signing up and creating an account is long and requires many steps. This negative effect of set-up cost on users' intention is consistent with the findings of other scholars [169],[172],[216]. Owing to the strong mooring effect of set-up cost, service providers should keep the set-up cost as small as possible, for example, by allowing users to easily transfer their accounts and passwords to the password manager, and simplifying the sign-up process.

Unexpectedly, the learning cost of using password manager applications is not a significant barrier to password manager adoption among smartphone owners. As many users now are using different mobile applications in their smartphones, offering various services compared to using desktop or web-based applications, users might be used to interacting with different types of mobile applications, so do not perceive that there will be a cost related to learning how to use a new one. Another explanation is that smartphone users can always find all the applications they need in one store, the 'Google Play Store'. This might give them the perception that any application in this store is designed to be easy to learn.

Similarly, the monetary cost is not a significant mooring factor for switching to a password manager. This might be due to the fact that some password manager applications are available free of charge. Moreover, since the application is dealing with passwords, users might not trust the free versions of these applications, due to the common belief that the true cost of free services is the user's privacy.

Another obstacle of adopting password managers is users' perception of the potential risk of using password managers. Users' perceived risk is an important barrier for users who are con-

sidering whether to switch to password managers. In this study, perceived risk was defined as users' belief that if they use a password manager, they will suffer potential problems, such as losing their passwords. This perception appears to be related to security and privacy concerns. For example, users' concerns that the service providers can access their passwords accentuate their perceptions of the risks of using a password manager. Likewise, concerns over the security level of password managers and their ability to resist attacks contribute to individual risk perception. However, a comparison of both security and privacy concerns shows that security concerns have a greater impact on users' risk perceptions than privacy concerns. These findings are similar to those of Yang et al. (2015) [207]. In a web-to-mobile shopping extension behaviour study, they concluded that the perceived risk of mobile shopping services might be an important factor in explaining the intention to install a mobile shopping extension. In addition, according to a study by Gumussoy et al., when users perceive mobile banking to be risky and insecure, their intention to use mobile banking decreases [206], consistent with the findings of this study.

Research Implications

The research has some practical and theoretical implications. First, the study employed Migration theory to examine the factors affecting security behaviour from different perspectives: pull, push and mooring factors. The research provides theoretical insights for researchers, which may assist in encouraging researchers to view security behaviour in a wider lens, and consider users' existing behaviour, as well as the new recommended one. Second, the results of this study reveal some important factors related to password managers and users' adoption decisions, which have not been addressed by previous studies. This study suggests that service providers and security advisors should consider focusing their promotion strategies more on establishing trust in password managers. For example, the source code of a password manager could be open and available to anyone to review. Additionally, the cost of migrating accounts and passwords should be considered. Developers should focus attention on the cost of setting up a password manager, for instance, by making the import of existing accounts smooth and easy, instead of requiring people to move them one by one. Illustrating the usefulness of password managers, compared to not using them, and their effectiveness in protecting online accounts safely could attract more users to adopt them. The power of social influence can also be utilised to encourage more users to switch to password managers.

Summary

The findings show reasons for users to switch to a password manager in two aspects. First, their dissatisfaction with their current password coping strategies appears to be a push effect, and encourages users to change their method. Second, it has been found that relative usefulness and perceived response efficacy have a pull effect, attracting users to switch to a password manager. In addition, the normative influence appears to be a facilitator that promotes password manager

switching behaviour. However, password manager switching is "moored" by the direct influence of the switching costs and the perceived risk of using this tool. Switching costs act as a barrier to password manager migration. The set-up cost specifically hinders users from switching to a password manager. However, the results suggest that the learning and financial costs are not significant barriers in the context of adoption of password managers among smartphone users. Moreover, the perceived risk of using a password manager is a significant obstacle that deters users from adopting this application.

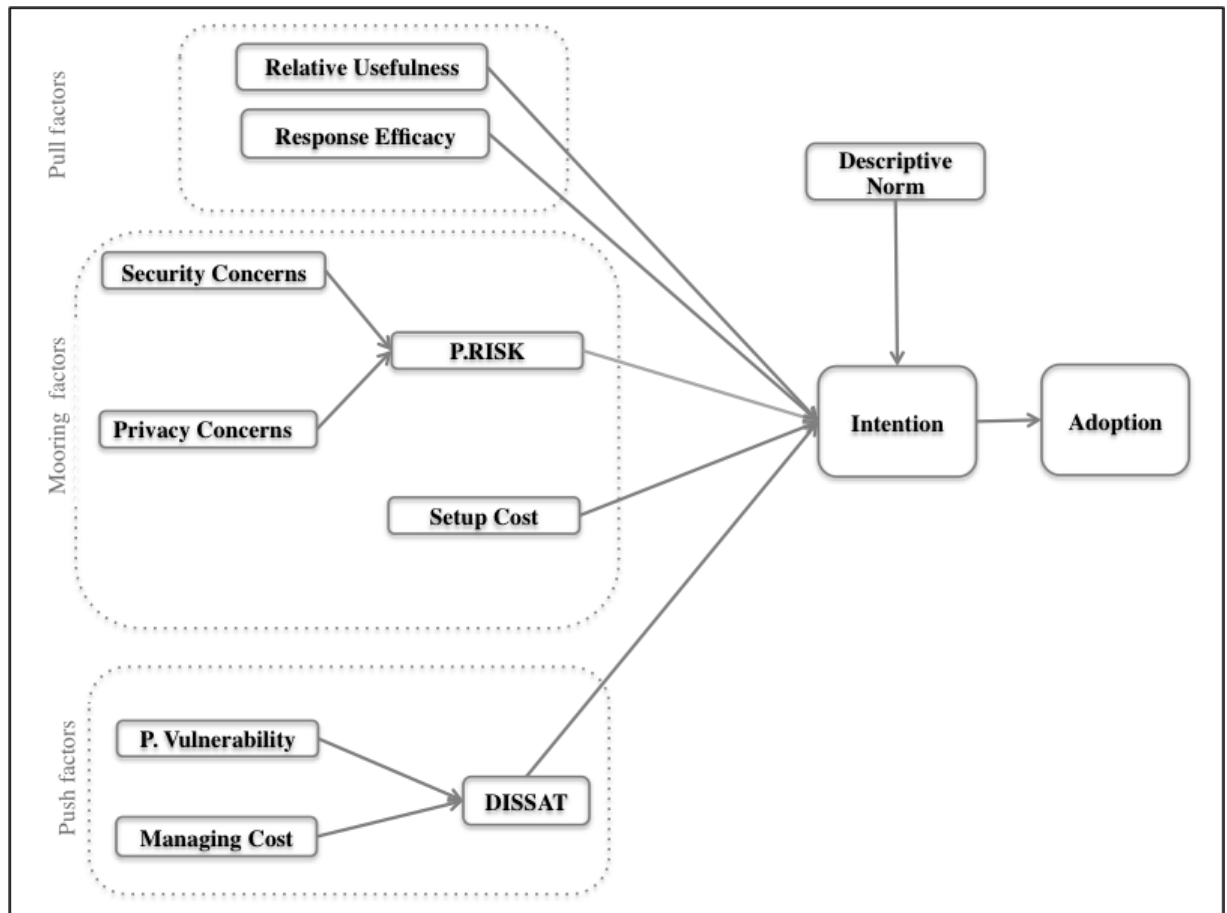


Figure 5.3: Password manager migration final model

5.8 Conclusion

A password management application is one of the most promising solutions for the problem of password security and usability. The initial factors affecting adoption decisions with regard to password managers were identified based on semi-structured interviews, and confirmed using an app as a survey harness. The study employed Migration theory as a theoretical lens to explain smartphone users' switching behaviour to the password manager. Through SEM analysis, six factors were found to be significant in predicting users' willingness to adopt a password man-

ager: descriptive norm, relative usefulness, response efficacy, dissatisfaction, perceived risk and set-up cost. This study has contributed to the information security field by applying Migration theory to understand security tool adoption behaviour. Furthermore, the study also confirmed that the intention to perform a security behaviour predicts actual security behaviours in this context. The study can also provide guidance to service providers and security advisors in effectively promoting the adoption of password managers. However, this result may only be generalisable to android smartphone users.

Chapter 6

Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs

6.1 Introduction

This chapter reports on the impact of a recommender application that harnesses the tenets of self-determination theory to encourage the adoption of password managers. This theory argues that meeting a person's autonomy, relatedness and competence needs will make them more likely to adopt a recommended behaviour. To test the power of meeting these needs, a factorial experiment was conducted in the wild. The recommender application supported each of the three self-determination factors individually, and all individual combinations thereof, and the short-term adoption of password managers was observed. The Android recommender application was used by 470 participants, who were randomly assigned to one of the experimental or control conditions. The analysis revealed that 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.

6.2 Study Aims and 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 encouraging observable short-term adoption of a password manager. 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.

As reported in Chapter 3, actual password manager adoption comprises three stages: (1) search, (2) decide, and (3) try - the latter being indicative of short-term adoption. A recommender appli-

cation will support users in searching and deciding, and then allow seeing whether a trial ensues. Hence, the following hypotheses were formulated and a user study was designed accordingly. This study is concerned with determining short-term adoption (i.e. the 'try' stage).

6.2.1 The Impact of the Recommender System

The first two hypotheses are related to whether the recommender system, which suggests a password manager to the user, makes a difference in password manager adoption.

Ha0: There is no difference in password manager adoption between participants who use a recommender system, and those who are merely informed of their existence.

Ha1: 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.

6.2.2 The Impact of Needs Satisfaction

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

Hb0: A recommender application that meets a participant's autonomy, competence and relatedness needs does not change the incidence of password manager adoption.

Hb1: A recommender application that meets the autonomy need significantly increases password manager adoption.

Hb2: A recommender application that meets the competence need significantly increases password manager adoption.

Hb3: A recommender application that meets the relatedness need significantly increases password manager adoption.

Hb4: A recommender application that meets the competence need significantly increases password manager adoption only if the autonomy need is also supported.

Hb5: A recommender application that meets the relatedness need significantly increases password manager adoption only if the autonomy need is also supported.

Hb6: A recommender application that meets the relatedness need significantly increases password manager adoption only if competence need is also supported.

Hb7: A recommender application that meets the relatedness need significantly increases password manager adoption only if the competence and autonomy needs are also supported.

6.3 Intervention 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 suitable one. Users were thus offered 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 to test self-determination theory-based interventions. The recommender supported users during the searching and deciding stages involved in password manager adoption (Chapter 3), and then observed whether they proceeded to the trial stage (i.e. installed a password manager).

6.3.1 Raising Awareness

The recommender's first role was to raise awareness of password managers. Chapter 3 reported that people are generally unaware of password managers, so an awareness video was included in the intervention. The awareness video clip used in the study of Aurigemma et al. [258] was used.

This video provides an overview of password managers, and the reasons for using them, and details the attractive features of such tools, such as their 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, the application proceeded to support the searching and deciding stages.

6.3.2 The CyberPal Recommender Application

CyberPal was implemented as an Android smartphone application. The user selects a number of preferred password manager features. The recommender system then suggests one or more matching password managers for consideration, based on their selected features.

a. Password Manager Features:

The interviews (mentioned in Chapter 5) were used to identify the features that users deem most important in a password manager when searching for one. Therefore, all statements about features provided by password managers or any desired characteristics of these applications were extracted. Hence, 13 features of password managers were identified. These features are:

1. **Open Source.** An open source application is one that is available along with its source code for open community development and review. Since a community of people are dedicated to keeping it secure and continually reviewing and improving it, it can be a trustworthy application. Due to privacy concerns, some users are reluctant to use a password manager. Having the source code of a password manager open and available for review increases the trustworthiness of these applications. Some users in the interviews expressed doubts over whether password manager developers can access their data, and suggested that if a third party can review the software, this would convince them to trust it:

“if we can check the software.. I mean not me.. [...] yah other programmers then we can trust that software more”

Other users stated that finding an open source password manager would make it possible for them to start using a password manager:

“if it is an open source application”

Therefore, an open source password manager might be a good option for users who are reluctant to use such applications due to trust issues.

2. **Security Company.** Due to the secrecy of the password data and users' perceptions of the potential risks of using a password manager, the availability of a password manager from a well-known dedicated security company would convince them to start using it. Interestingly, participants trusted the security companies that have popular anti-virus software, such as McAfee:

“a well-known company like anti-virus companies for example McAfee”

This might be because users trust these companies in catching any virus in their device, and hence would trust a password manager from such a source.

3. **Two-Factor Authentication.** Two-factor authentication is a term used to describe an authentication method where two different factors are required to authenticate a user. For

example, a password and Yubikey device, or one-time authenticator. It is an effective mechanism to protect online accounts, hence it can improve the security level of cloud-based password managers. It was suggested by some interviewees that multi-factor authentication should be used in password manager applications:

“some more kind of maybe multi-step process...if a multi-step process is used maybe I would consider it.”

Therefore, some users may prefer to choose a password manager that can be protected with a second authentication factor.

4. **Fast Access.** Since the master key is typically complex and long, some users find it difficult to type each time they want to access their online accounts. To simplify the password manager experience, many password managers offer an alternate fast way to log into the password manager, such as a 4-digit passcode or Touch ID. Some interviewees suggested having this feature in a password manager:

“just quick access. Maybe some of the phones with thumb-prints..things like that”

Users can enable these features in their devices to easily access their password manager application.

5. **Synchronisation.** Synchronisation is about propagating passwords changed on one device to all other devices. Many users use multiple devices, such as smartphones, tablets, laptops or desktop computers, to access their online accounts. Hence, they need to save their credentials on all of their devices. In the interview, users mentioned password synchronisation as an advantage of using a password manager:

“it can work across devices as well.”

It is expected that some users would seek this feature when searching for a password manager.

6. **Safe Sharing.** For some colleagues and partners, password sharing is used as a practical means of managing collaborative work, financial management, or a demonstration of trust. Users were wondering whether they could share passwords while using a password manager:

“I got married just recently, so my wife[...]we share some accounts ,like on-line banking for example...I am not quite sure how this would work with the password manager”

End users might need to share some of their passwords with others. Thus, many password managers provide functionality to safely share passwords with others. Sharing passwords was thus added as a desired feature when searching for a password manager.

7. **Security Feedback.** It is assumed that people use a password manager to improve the security of their stored passwords. Therefore, some users like to find a password manager that provides insight into their passwords’ security. They described their need to assess the security of their stored passwords:

“it would be quite good if there was a separate list that was like you use, like,... obviously encrypted, but if it was a list of the passwords you use and then you click on that and it gives you all the websites. Cause then I’d be able to see, oh, I’m using that one [password] way too much”

This feedback can inform users about the strength of their passwords, and whether they have been reused in another login, providing the opportunity to improve their security.

8. **Location Access Restriction.** As mentioned earlier, due to the secret nature of passwords, people take extra care when choosing a password manager to assess its security level compared to other applications. Some users liken it to banking, and want to see the same precautions in a password manager as those applied by banks, such as restricting transactions to a specific region, and warning users when transactions are requested outside that geographical location:

“ might send me an email says that you login into a different location which is not usually the one you log in from. So, it just like you know when you withdraw money from your bank from overseas, the bank always sends you an email or a message say ‘oh’ your bank account has just withdrawn this amount from this country. If you have any concern then call us”

Some password managers offer the feature to restrict access to passwords from specific locations. It was decided to add this feature to the recommendation system.

9. **Audit (Track).** Similar to location access restriction, some users suggested adding a tracking feature to log any activity in the password manager. They described their need to be informed about any activity made via their account:

“Tracking for unusual logging. They can track for logins and when I see a login and I am actually not logging in I will say oh that’s not me something wrong happen and I contact them. Like in my gmail every time I try to login from a different device they send an email says someone trying to access your email from a MacBook computer”

Tracking is the process of logging the activities related to accessing a password manager. This feature can give the user a sense of control over the security of their passwords. Therefore, another security feature that was added to the recommendation system is activity tracking.

10. **Cloud vs. Local.** Users have different preferences regarding where to store their encrypted passwords: in the cloud or locally on their device. Cloud-based storage offers many advantages for users, such as access from anywhere, at any time. Thus, some users would prefer to use a cloud-based password manager:

“it’s better to save them on the cloud”

Interestingly, however, other users favoured keeping their passwords only on their devices:

“I really don’t like to keep them out of my phone”

Therefore, the choice of cloud storage or local storage was provided in the recommendation system.

11. **Free.** Some users would look for a password manager that is free of charge:

“if it was free and well-reviewed”

There are many free password manager applications. Some offer a free version and a premium paid version with extra features. Therefore, this feature was added to the recommender system.

12. **Export Passwords.** This is the process of transferring a copy of the data from the password manager to secure storage for safekeeping. Users want to have control over their passwords stored in the password manager. They wondered whether they could stop using the password manager and keep their passwords:

“last time I drop my phone in the water and it did not work anymore. So I am thinking of what could happen if I am using a password manager. I am

thinking what if I lost the passwords for everything. So that is kind of a risk if I am actually using a password manager”

The suggestion was made to add a feature to export passwords to a backup in order to guard against any failure. Thus, the export passwords feature was added to the list of features in the recommendation system.

13. **Master Key Recovery Support.** Some users were concerned about forgetting their master key and being unable to access their accounts:

“what about if I forget the master key?”

Some password managers offer an option for the user to provide a hint that can remind them of the master password. This hint can be displayed or sent to the user on demand. Therefore, this feature was included in the recommendation system.

← Explore Password Managers

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 ⓘ

☐ Location Access Restriction ⓘ

☐ Track Activity ⓘ

Recommend a Password Manager

Figure 6.1: Password manager features in CyberPal

b. Order Preferences

As it is difficult to find an available password manager that satisfies all requirements, users were asked to order their preferences based on the chosen features, from most preferred to least preferred feature (Figure 6.2). Then, the recommendation application calculated the utility value of each of the password managers by adding the rank value of each feature, if available in the

password manager, or adding zero, if unavailable. The system, then, suggested one (or multiple) password manager(s) with the highest utility value for that user.

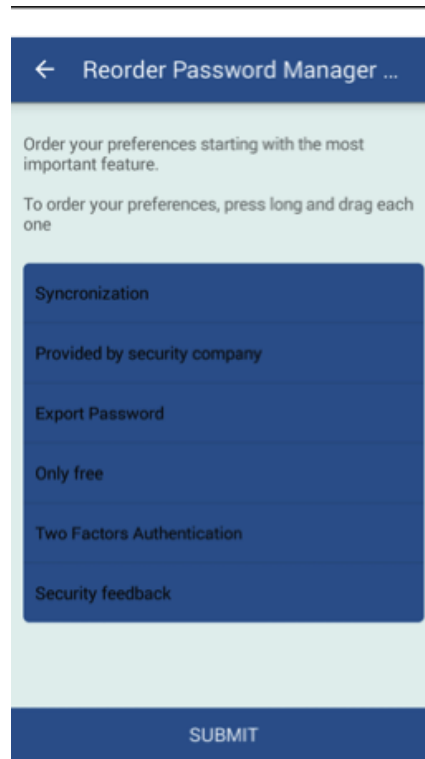


Figure 6.2: Order preferences

c. Password Manager Applications

To design the recommendation system, 16 password manager applications were carefully selected based on expert recommendations [260], [261] - those that offered combinations of the features mentioned in section 6.3.2. All these applications were highly rated in the Google Play Store, with at least 4.3 stars. These applications were tested, using dummy accounts, to ensure that they worked without any technical problems. These applications are: KeePass2Android, PasswdSafe, Bitwarden, keepassDroid, LastPass, Enpass, DashLane, KasperSky, Padlock, Zoho, Norton, Roboform, 1Password, TrueKey, Keeper and Encryptr. The password managers' names and their associated features were recorded in a database. If a particular feature existed then '1' was recorded; otherwise, if the feature was absent, '0' was recorded.

d. Supporting Self-determination Needs

Features were added to the recommender to support 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 [189], [263], [175],[173]. The recommender system was tailored to meet these needs, depending on the experimental condition to which the participant was randomly allocated (more details about the experimental groups can be found in

experimental design, section 6.4).

Autonomy. Different strategies have been suggested to support autonomy. For example, the use of non-controlling language [266], [267], acknowledging negative feelings [267], [268], and offering more than one option from which the person can choose [189], [267]. It has been suggested that offering three options is sufficient to create an autonomy-supportive context [269]. The autonomy need is supported in CyberPal by using two strategies: (1) offering choice, and (2) using non-controlling language. Regarding non-controlling language, words such as "would you like..." and "you may..." are used. Furthermore, providing more than one choice engenders a feeling of autonomy, but too many choices can create a potentially negative effect [270]. Therefore, CyberPal offered participants a choice of three password managers to support the autonomy need; each of them links to the application on Google play store [169](Figure 6.3).

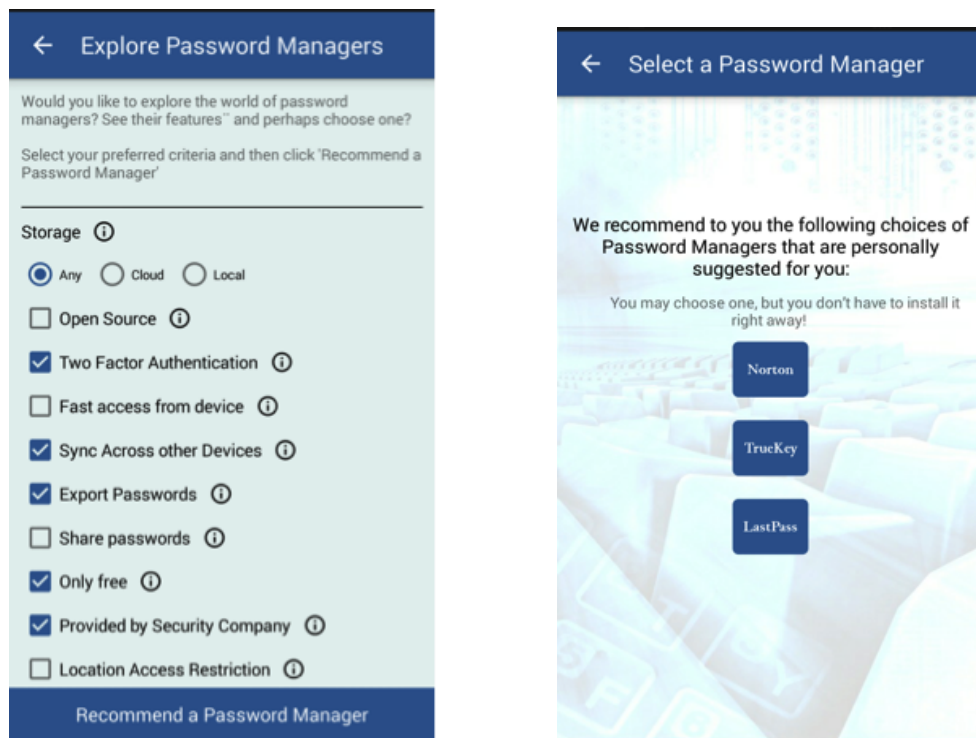


Figure 6.3: Supporting autonomy in the recommender app

Relatedness. The relatedness need can be supported by providing some kind of connectivity related to the target behaviour [271]. This may constitute the provision of a community environment or a communication channel [272]. During the pre-adoption stage, being aware of other password manager adopters can support the relatedness basic need in this context [273]. Because password managers are critical systems, and relatively poorly known, being aware of the fact that your contacts are password manager adopters may give the CyberPal users a feeling that they are not alone. This can support their relatedness need. CyberPal thus highlights con-

tacts who are using a password manager (Figure 6.4 and Figure 6.5). This was implemented by retrieving all the contacts in users' device. Then connect between their phone numbers and the CyberPal users' phone numbers used in the registration. If the user has a password manager in her/his device, this was highlighted as shown in Figure 6.5.

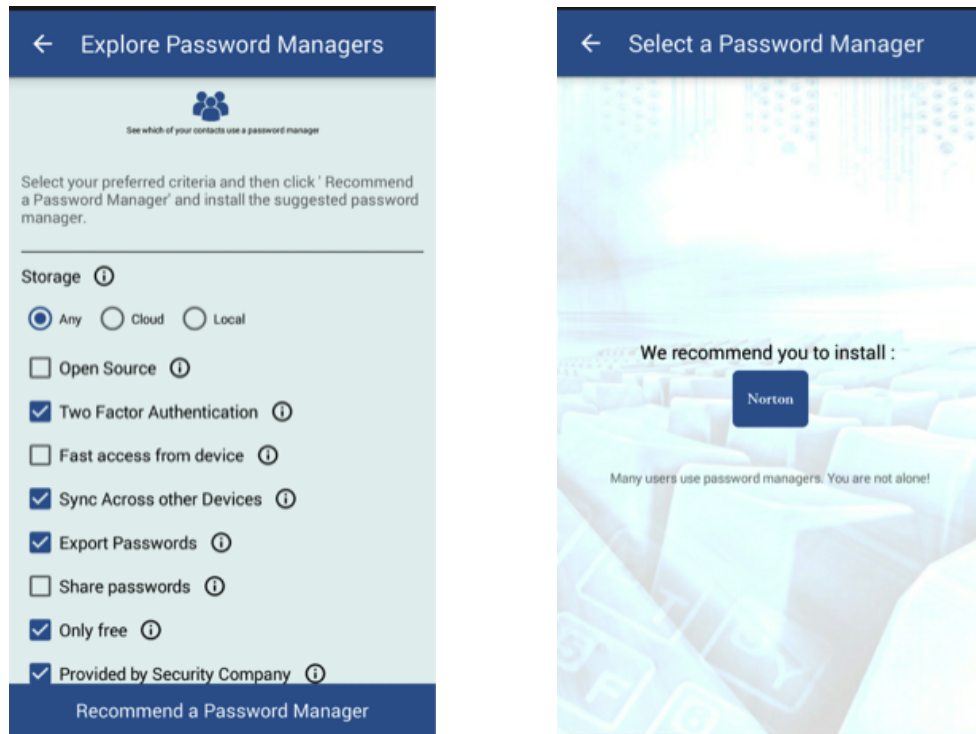


Figure 6.4: Supporting relatedness in the recommender app



Figure 6.5: Supporting relatedness-who use a password manager in your contact

Competence. Suggested strategies for meeting this need include: (1) offering clarity [274], (2) using positive feedback [275],[276], (3) providing guidance [274], (4) encouraging individuals, and (5) supporting their perceived capabilities where their belief that they can perform the target behaviour causes them to anticipate that they will perform the activity without assistance [277]. A person might like the idea of a password manager, and want to use one, but be uncertain about possible future scenarios. They may be concerned about what would happen if they replaced their device or installed an operating system update. This uncertainty could compromise their feeling of competence and deter them from trialling a password manager. CyberPal provides a "frequently asked questions" button to enhance clarity and answer questions about a range of scenarios, in order to reduce uncertainty. The competence need is also satisfied by providing a positive feedback message when the users submit their preferences, to encourage them to proceed with the installation of the recommended password manager. Also, CyberPal provides information about the most desired features chosen by other CyberPal users: the percentage shows how popular each feature is amongst other CyberPal users (Figure 6.6).

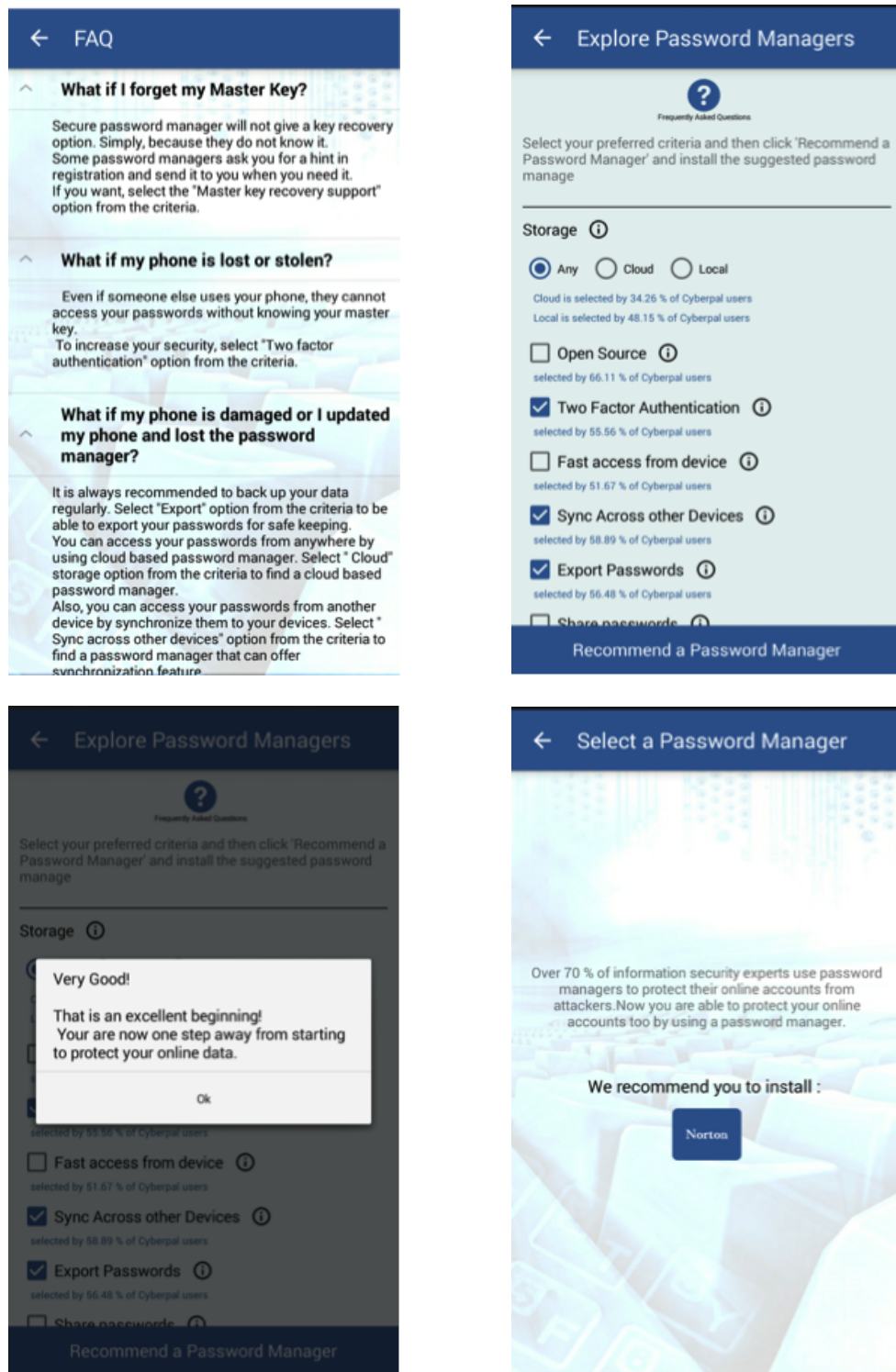


Figure 6.6: Supporting competences in the recommender app

Table 6.1: Supporting Self Determination Needs in CyberPal app

The Basic need	From the Literature	From the interview	Strategy to support in the intervention design
Autonomy	Provide choices, [189] [263] [175], Use non controlling language [189],[263], Provide relevance and meaningful reasons for users' action [189] [263]	"I want to choose where to put my passwords"P3	Autonomy was supported by suggesting to the user three choices of password manager applications instead of only one. Use of non-controlling language. e.g. "would you like.." , "you may" , and "personally suggested"
Relatedness	Create community [268], Provide channel for communication [268], Provide updated news [268]	"I dont want to be first" P6 "When I knew that some of my techy friends are using it, I am going to use it as well " P10	Give the users the chance to view whose in their contact are using password manager application. The availability of this feature should give the user a sense of being part of a community.
Competency	Intuitive interface [175],[173] Knowledge and, guidance [262], [173], [263], Provide Feedback [262],[263]	"What about if I forget my master key?!", P18	Overcome any ambiguity or uncertainty that might concern the user by using frequently asked question in the application. User receives positive feedback after submitting their choices. Provides a message under each feature that shows the percentage of how popular each feature.

e. 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, compared to other smartphone operating systems [278],[279].

6.3.3 Behavioural Intention

As mentioned in Chapter 3, 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. However, using CyberPal might help a person to formulate an intention to use

a password manager. Furthermore, because the experiment was conducted in the wild, it was expected that some participants would have perfectly valid reasons for forming a low, or no, intention to use a password manager. Thus, behavioural intention was measured in the pre-questionnaire in order to measure the participants' intention to install a password manager in the coming week, on a 7-point Likert scale [283]. In the pre-questionnaire, the participants were asked for their gender, age and education. After a week, a post-questionnaire popped up, asking the participants to select reasons for choosing to use a password manager, or not, as the case may be. Also, they were asked to rate the importance of a set of password manager features.

6.3.4 Testing

During the development process, the CyberPal application was tested extensively on 12 Android devices to assess and improve it. The application was then tested by a sample of 6 Android users to improve its usability. Finally, the application was uploaded to the 'Betafamily.com' testing service, where it was tested by 9 testers over a two-week period. Their comments and feedback were used to improve the application.

6.4 Data Collection

6.4.1 Experiment Design

The experiment allowed testing for the following:

1. The effect of the password manager recommender system compared to only providing information about a password manager (Hypotheses Ha (0,1)), and
2. The effect of supporting the three SDT needs, exhaustively testing all possible combinations (Hypotheses Hb (0,1-7)).

To avoid the experimental hazard of the participants expecting to install a password manager, a placebo condition was included, i.e. an intervention that had no effect. In psychological experiments, researchers generally utilise a placebo group: a group of participants who are exposed to a placebo or fake independent variable [280], [281], [282]. The impact of this non-intervention is then compared to the results of the real independent variable of interest. This strategy is often used in social science experiments where the avoidance of external conditions is impossible. This seemed advisable for this experiment too. In the placebo case, CyberPal merely displayed information about password manager tools, as extracted 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 sat-

ified some combination of the three SDT needs. Participants were randomly assigned to one of the experiment groups or the placebo control group (Table 6.2). This type of design can help to establish causation by determining cause and effect between variables. Also, it can isolate the impact of each intervention on adoption behaviour and determine which of the three independent variables, or their interactions, are more likely to influence adoption.

Table 6.2: Description of the experimental groups

Group Code	Description of the CyberPal version
G1	List of password managers without recommendations (placebo)
G2	Recommendation satisfies autonomy need
G3	Recommendation satisfies competence need
G4	Recommendation satisfies autonomy & competence needs
G5	Recommendation satisfies relatedness need
G6	Recommendation satisfies autonomy & relatedness needs
G7	Recommendation satisfies competence & relatedness needs
G8	Recommendation satisfies autonomy, competence & relatedness needs
G9	Only a recommendation system without features designed to satisfy needs

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 established 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.



← Explore Password Managers

Here are some password managers available in google play store :

Password Manager	Rating
KeePass2Android	4.7
PasswdSafe	4.7
Bitwarden	4.7
keepassDroid	4.6
LastPass	4.6
Enpass	4.6
DashLane	4.5
KasperSky	4.4

Figure 6.7: Group 1-placebo interface

6.4.2 Ethical Considerations

The data that was collected in the mobile application is privacy sensitive, and great care was taken to respect participants' privacy. The study was conducted under the approval of the University of Glasgow institutional review board. The participants' consent was obtained before collecting any data. Only the aggregate statistics were reported, thereby ensuring participant anonymity (more detail is available in Appendix C).

6.4.3 Task

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 with 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.

6.4.4 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, the 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 this study, there was a need for 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 the participants who completed their tasks entered the prize draw. The winner of a £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.

6.4.5 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 smartphone 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 [283]. Self-reported responses were recorded on a 7-item Likert scale: 7 means high intention to use a password manager, and 1 indicates low intention.

6.5 Analysis

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

63.8% of participants were male, while 34.6% were female. The majority of the participants were aged under 45 years. These statistics are consistent with AdMob's survey on smartphone owners indicating that 73 percent of Android smartphone owners are males and the majority of Android owners are under 44 years old [265].

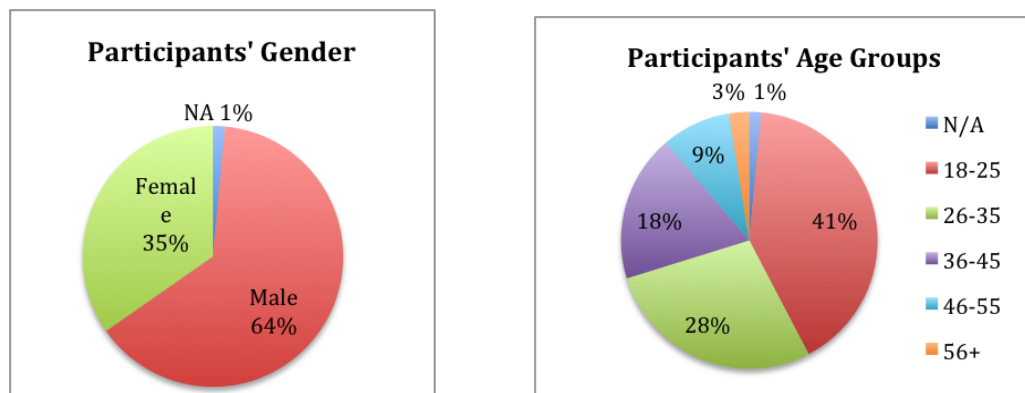


Figure 6.8: Participants' demographics

The analysis shows that the participants have various education levels. It has been observed that the majority of them reported having a Bachelor's degree or less while 14% held a higher education degree (Figure 6.9).

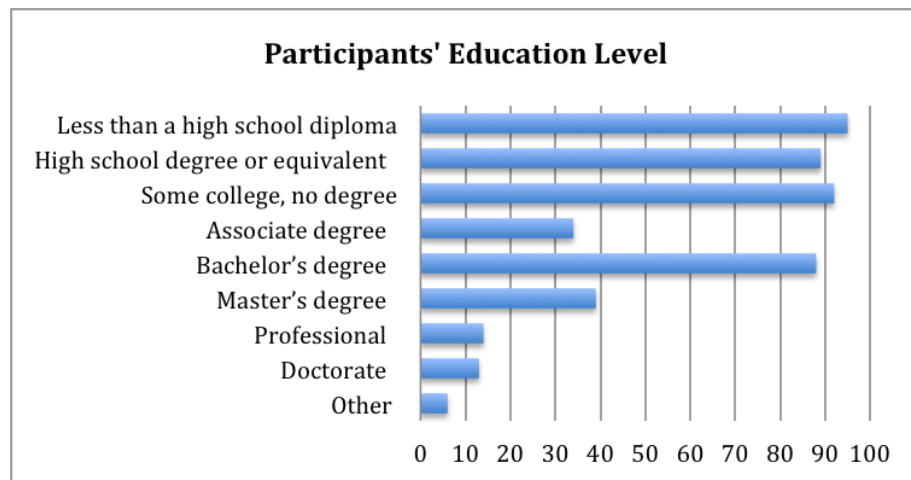


Figure 6.9: Participants' education level

In this study, the participants were asked about their current method for managing their passwords, and they could select all the applicable options. Figure 6.10 summarises the selected responses by the respondents. The most commonly used coping method was to use similar passwords with a slight change to the main password. Using the same password to access multiple accounts was the second most commonly used method. 30% of participants reported that they used personal information such as a pet's name or date of birth to remember their passwords, while 17% indicated that they save their passwords in their browsers. Similarly, 17% of the subjects reported that they recorded their passwords in a notebook.

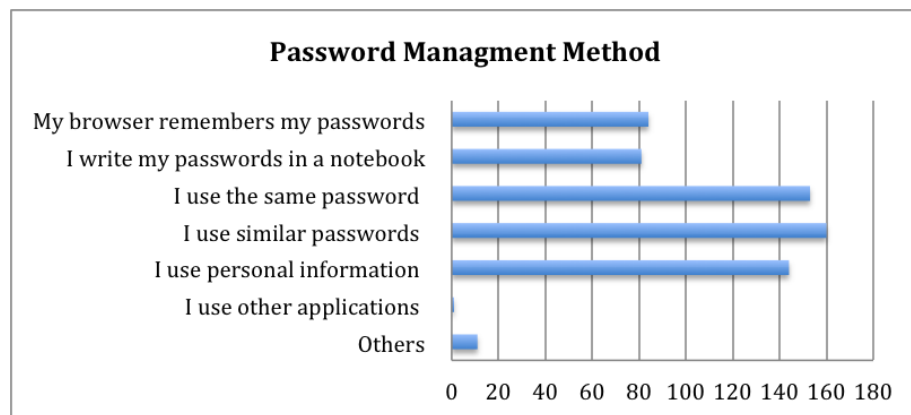


Figure 6.10: Participants' methods for managing their passwords

When investigating whether the participants were previously aware of the existence of password manager applications, the result indicates that 42% of them were aware of them, while 58% reported no prior awareness.

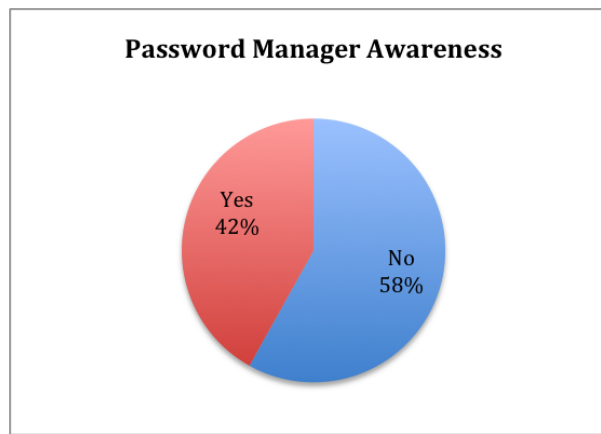


Figure 6.11: Participants' awareness of password manager

To explore their information technology experience, the participants were asked to rate their IT skills on a 7-point scale. Furthermore, they were asked to rate their information security knowledge from 1 to 7. Only 22% of the participants rated their IT experience lower than 4, meaning they can be considered as novice users. Yet, despite this low ranking, nearly double at over 37% of them rated their information security knowledge lower than 4. The average rate of IT experience in this study was 4.43 while it was 3.75 for security knowledge. Among users who were aware of password managers, the mean rate was 5.29 and 4.33 (for IT skills and security knowledge, respectively) compared to 3.80 and 3.31 for the group who were not aware of password managers.

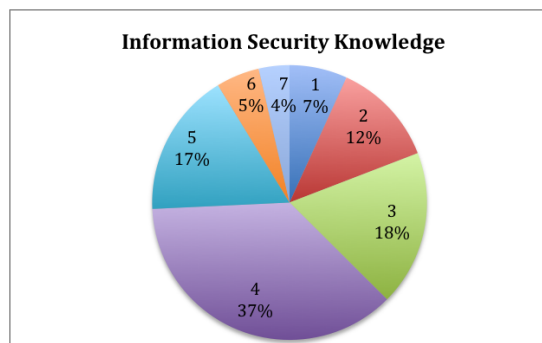


Figure 6.12: Participants' IT skill level

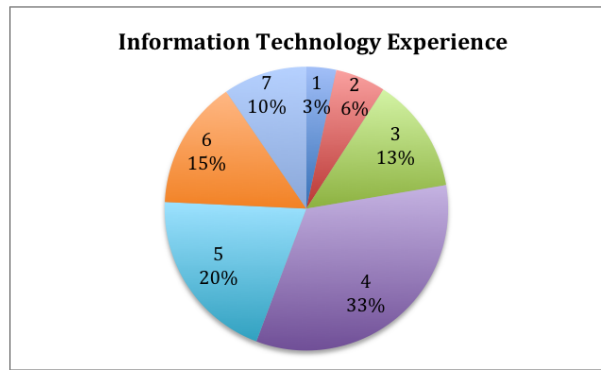


Figure 6.13: Participants' information security knowledge

Table 6.3 shows that the mean values of the intention are relatively similar across the groups ranging between 4.36 and 4.63; although it is slightly lower in Group 3 (4.14). The sample size in each group is slightly different, an inevitable side effect of random allocation in the wild.

Table 6.3: Descriptive Analysis

(PM=Password Manager)

Group Code	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)

Inferential statistical tests were conducted using SPSS version 24 to test the hypotheses (Section 6.2). To test these 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 (0,1-7).

6.5.1 Testing the Impact of the Recommender Application

The first step was to compare groups that used the recommender system, and the control group. A cross-tabulation 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 X^2 test was conducted to determine whether there were significant differences in adoption behaviour between the participants in the two groups. The X^2 statistic is 5.609. 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 and the group that merely enhanced their awareness. Thus, the null hypothesis (H_0) 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 cross-tabulation test, the alternative hypothesis is accepted (H_1).

6.5.2 Testing the Impact of SDT Need Satisfaction

Table 6.3 shows that when the three needs were satisfied (G8), more participants adopted password managers than in the other groups. This is followed by the case when Autonomy and Relatedness needs are met (G6). A further step is needed to determine which factors exercised the greatest influence. First, three variables A, C, and R, representing 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 [263], therefore it was added as a control variable. As Table 6.4 shows, only relatedness and autonomy significantly influence 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 (G2, G3, G4, G5, G6, G7, G8 and G9) with respect to password manager adoption rate, X^2 tests were used. The null hypothesis (H_0) can be rejected.

Table 6.4: Binary Logistic Regression

(A=Autonomy, C=Competence, R=Relatedness) * Significance Starred

Variables	Group	β	Std.Err.	p
Intention	-	.915	.110	.000*
A	G2	1.099	.511	.031*
C	G3	.285	.562	.613
R	G5	1.046	.514	.042*
A*C	G4	-.218	.723	.763
A*R	G6	-.956	.685	.163
C*R	G7	-.216	.732	.768
A*C*R	G8	.423	.965	.661

6.5.3 Reasons for Adoption Decision

To understand why the participants chose, or did not choose, to install a password manager, a post-questionnaire was presented that popped up a week after they had installed the app. They were asked: "Have you installed a password manager? ", with pre-defined multiple-choice answers. From 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 it but not yet used it; an expected result with a short term observation. The installing participants were asked about their main reasons for doing so (Table 6.5).

Participants who did NOT install a password manager were asked why they did not do this (Table 6.6). Overall, it was observed that most installing participants (90%) claimed to use a password manager due to the convenience it provided, whereas only (35%) indicated that it was installed for security purposes (Table 6.5). Of those opting not to install a password manager, a number of participants believed that setting up a password manager took too much time (30% of 331) and 26% preferred to wait until password manager applications became more popular amongst their close connections. Twenty-two (7%) did not install a password manager because they could not decide which one to install (Table 6.6). Interestingly, the majority of these belonged to Group 1, which confirms the importance of supporting end-users' decisions.

Table 6.5: Reasons for installing a password manager

Reasons	% (n=139)
To support my own memory (i.e. I can't remember all my passwords)	90%(125)
To use the auto-filling feature of user name and password when I login to my accounts	17%(24)
To keep my passwords synchronized across all my devices	37%(52)
To have a safe way to share some of my passwords	5%(7)
To improve the security of my passwords e.g use system generated passwords /use unique passwords for each of my accounts	35%(49)
To have a secure storage for important data such as credit card details	53%(74)
Other reason (Please specify)	1%(1)

Table 6.6: Reasons for not installing a Password Manager

Reasons	% (n=331)
Because of phone related issues (i.e. Insufficient memory space, the device is slow or the battery is consumed quickly)	8% (25)
Because it takes time to set up a PM	30%(98)
Because I don't trust my phone device to be free of viruses or malware. (e.g. hackers can spy on my phone and steal my passwords or compromise the PM)	10%(33)
Because my phone could get lost/stolen at any time	3%(10)
Because I don't trust PM applications, even if my friends or family members use them	19%(62)
Because I don't want to be the first one in my family and friends to use a PM application	26%(87)
Because I can't decide which PM application to use	7%(22)
Because I don't know how to use a PM application	4%(12)
Because I don't need a PM application	2%(5)
Other reason (please specify)	1%(4)

6.5.4 Password Manager Features

To understand the most preferred features of password managers, during the usage of the CyberPal app, users' selected choices of password manager features were recorded for all users (except from the control group users (Group1)).

The result (Table 6.7) shows that the most frequently selected feature of password managers was the open source code (66%). This was followed by applications that were developed by well-known security companies. Only 26% of the participants searched for a password manager that allowed sharing some passwords with other users. Interestingly, password managers with local storage were preferred more than the cloud-based password manager. Less than half of the subjects (42%) wanted password managers that were free of charge. Password managers that provide location access restriction as a security precaution were more frequently selected than those with an auditing security feature.

Table 6.7: The selected features in CyberPal

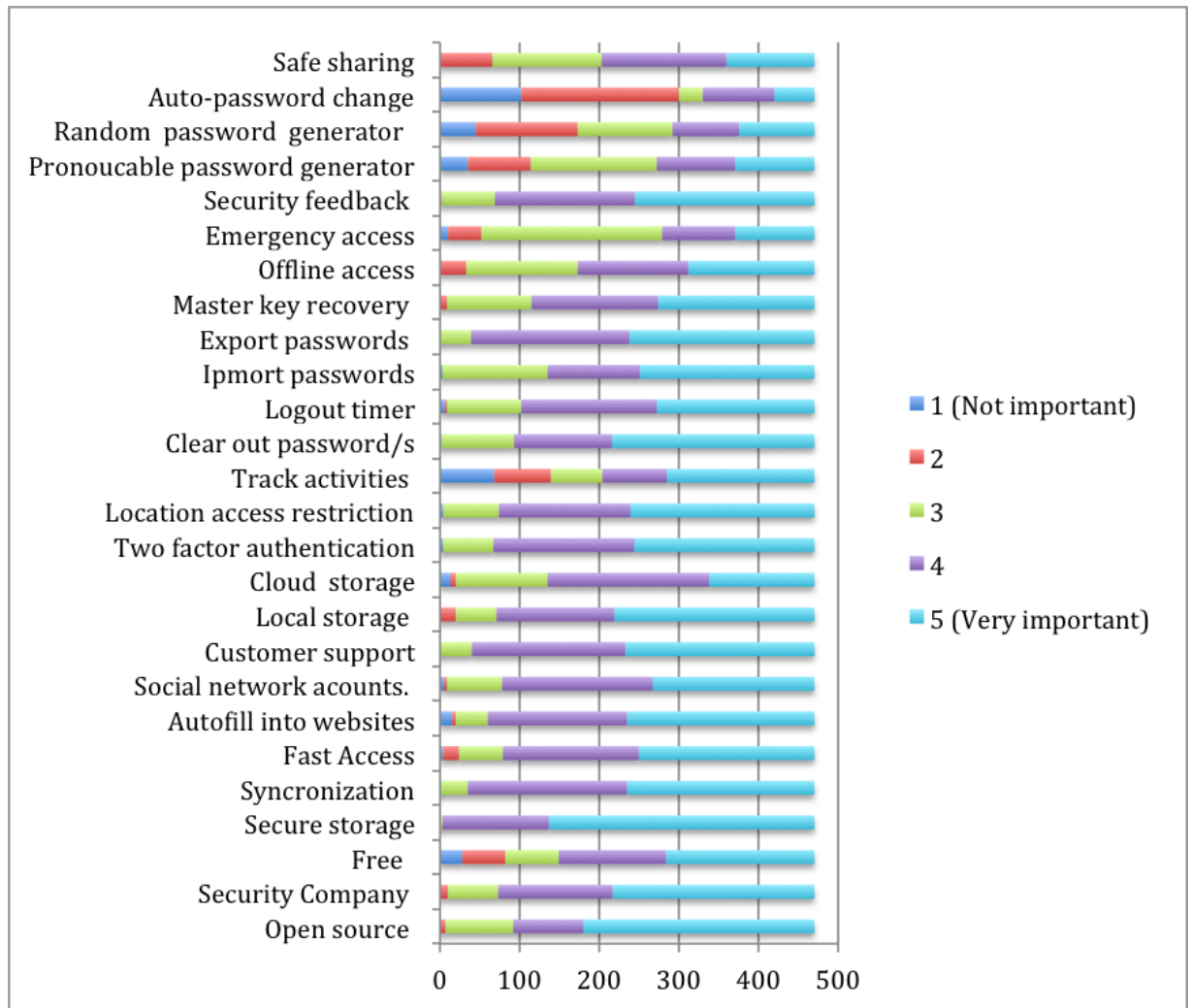
	Feature	%		Feature	%
1	Open Source	65.75	8	Security Feedback	51.02
2	Security Company	57.36	9	Fast Access	49.88
3	Local Storage	56.91	10	Master Key Recovery	44.44
4	Synchronization	53.28	11	Free	42.17
5	Export Passwords	52.60	12	Audit (Track)	41.95
6	Location Access Restriction	52.38	13	Cloud Storage	29.93
7	Two Factor Authentication	51.24	14	Safe Sharing	25.62

Furthermore, to understand the importance of password manager features, all users were asked to rate some features of password managers from 1 to 5 in the post-questionnaire; where 5 meant a highly important feature. These features were already found in some password manager applications that had been reviewed.

Looking at the rate of all the features in Figure 6.14, having secure storage for other types of data is by far the most important feature of password managers as 70% of the participants considered it to be "very important" on a five-point Likert scale. One can see that 61% or 290 of all the participants rated 'open source' with 5 (mean of 4.40). Both 'synchronisation' and 'communication channel for customer support' were rated by 50% of all subjects as a very important feature in password manager applications. This was followed by 'exporting passwords' with 49% rating it as very important and achieving an overall average of 4.41. The average importance rate of the free-of-charge password manager was 3.84 with 39.5% of the participants rating it as very important and 6% of them rating it as not important. Among the security precaution features, two-factor authentication and the location access restriction were the most highly rated security features. The average rate for the former was 4.32 with 226 (48%) participants assessing it as very important, while the mean rate for the latter was 4.31 with 231 (49%) ratings as a very important feature. This was followed by the log out timer (4.17 on average) while tracking activities ranked as the least important security precaution feature with 185 rating it as very important and 68 rating it as not important; the average rate was 3.52.

Surprisingly, password security features that are provided by password managers to improve password security levels were rated as the least important features. Only 10% rated an auto-password changer as a very important feature (with mean of 2.54), while 21% and 42% rated it with 1 (not important) and 2, respectively. Also, the random password generator was only considered by 94 participants (20%) as a very important feature of password managers, com-

pared to 45 and 128 who rated it as not important - scoring it with 1 and 2 respectively. The mean value of the pronounceable password generator was 3.31, which is slightly greater than the random password generator (3.11). The former was rated by 99 subjects as a very important feature (21%) while it was rated with 1 and 2 by 35 (7%) and 79 (16.8%) respectively.



(5= Very important, 1=not important) .

Figure 6.14: Respondent's rating of the features of password manager applications

6.6 Discussion

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.

Using a recommendation system:

The study found that a recommendation system is an effective intervention in encouraging the adoption of password managers, by facilitating the search and decide process preceding the adoption. It also suggests that 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.

It is acknowledged that the adoption process of a password manager, as discussed in Chapter 3, consists of searching and deciding before installing (trying). After a user becomes aware of password managers, and plans to use one, they will commence the process by searching for a suitable one. If they decide to proceed, a selection will be made from the proffered options. Supporting the user's search and decide decisions, by providing a recommender system, facilitates behavioural 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. For example, to prompt updates to a smartphone, users might be encouraged to think about the potential risks of losing particularly personal and sensitive data, such as photos or contact numbers. Providing an accompanying backup option, or explicitly ensuring that no data will be lost during the update, might improve update installations.

When comparing the intervention where users were given a recommender system with the intervention that notified users about the available password managers in the application store, the former resulted in more users installing a password manager. Therefore, the result shows that supporting users' decisions by providing a recommender system is important, to encourage them to adopt a password manager application. This corroborates the findings by Zanker et al. [264], who found a significantly larger share of availability requests was triggered by online visits to a tourism website that employed a knowledge-based recommendation system compared to the group of potential customers who did not use the system. Similarly here, when there was no recommendation system provided, participants were less likely to install a password manager.

Supporting SDT needs:

The nexus between SDT and the awareness intervention provided by the recommender app is an important contribution. 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. The satisfaction of three needs - autonomy, relatedness and competence - was experimentally manipulated within the context of recommending a password manager, in order 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 yields positive behavioural outcomes. Based on SDT's predictions, it was expected all of the three factors would have an impact on adoption. The 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 behaviour, the study explored the effect of two- and three-way interactions between the factors. However, no significant interaction effects were detected.

Relatedness: Some password manager providers already use word-of-mouth referrals by encouraging their users to invite other potential users. This study provides evidence of the effectiveness of such referral systems in encouraging adoption. Moreover, this 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 made suggestions in line with the users' own preferences.

Autonomy: Employing non-controlling language and providing choices to support autonomy successfully encouraged more users to adopt a password manager. Using assertive language (i.e. bossy) when advising 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. [262] 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, it is difficult to conclude from this study that the satisfaction of competence will always be insignificant. Two explanations suggest themselves for this result. 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.

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. Also, using a password manager as a secure storage for other types of data was an important reason for installing it. Since the password manager is mainly recommended to improve passwords' security level, it was not expected to find only 35% stating that they had installed a password manager to improve the security of their passwords. The study also found that one of the barriers to installing a password manager was the time it takes to set it up. Developers need to minimise password manager set-up times. Moreover, the popularity of password managers among small groups of users can convince more users to adopt these tools.

Password Manager Features:

To give more insight into users' preferences with regard to the features provided by most password managers, users were asked to rate the importance of a set of features on a 5-point Likert scale.

Among the security precaution features, two-factor authentication and location access restriction were the most important security features from the participants' point of view. These features are, especially, effective for the cloud-based password manager. The second most important security precaution feature was the ability to set up a timer for logging out from the password manager. This may be of importance in the case of losing the device. Although activities auditing and location restriction can both collect information about the user's location, tracking activities was rated as the least important security precaution. This might be due to the effort required from the user to check the log and assess the risk before taking a decision; compared to the location restriction, which does not require further checking after setting it up. Further, providing an explicit function for clearing data was highly rated as an important feature (Figure 6.14). Since users will be able to delete their passwords whenever they want, this feature may maintain their feeling of control over their passwords; especially non-tech-savvy users. For example, they can use it to ensure their passwords are completely deleted from their smartphones when they want to sell their devices or stop using a particular password manager.

As mentioned earlier in the reason for adoption decisions, the provided features for improving passwords' security were the lowest rated features. Although changing passwords regularly is recommended to minimize the risk of cyber security attack, this feature was the lowest rated feature among all the features. This finding was unexpected and it is not clear whether the reason for this low rate is the users' lack of awareness of the importance of changing passwords regularly or they do not favour this feature; even though the password manager would take away the burden of recalling these passwords. The random password generator was rated lower than the pronounceable password generator. This might be due to users' feeling of being able to remember pronounceable passwords compared to random ones. However, both features were not highly rated. Again, this was unexpected, given that the password manager would store these passwords anyway. Similarly, not all participants rated the sharing passwords feature as an important feature. This might be due to their low perceived need to share passwords, usually with partners. People would not find sharing passwords an important feature in a password manager unless they encounter a situation where they need to share a password with another person. Unlike password security features, providing users with feedback that assesses the security of their passwords had a high rate. It seems that instead of providing tools for improving passwords, users only need to be informed about the security level of their passwords and whether they are secure enough or not. Besides, unlike password generators and changers, this feature can

support users' motivation to master their security skills in creating a secure password.

Furthermore, the participants rated exporting passwords as a highly important feature. This feature can support users' feeling of control over their passwords. They might perceive that they can stop using the password manager whenever they want without losing their passwords. Importing passwords was, also, highly rated as an important feature. This feature can support the user to set up password manager when moving their passwords from the browser or another password manager application.

Having a communication channel for customer support such as live chat was amongst the highest rated features. Also, social network accounts were highly rated. These two features can provide support to the users in case of any query. Also, they keep users up-to-date with the potential news or issues regarding the password manager; hence they might have a positive impact on trusting these applications.

Interestingly, having a local-based password manager was more important than a cloud-based one. This might be due to privacy concerns as the cloud-based application stores the encrypted passwords outside the user's device. This can also explain the high rating of open source password managers. Furthermore, having a password manager developed by a well-known security company was considered an important feature. It seems users need an assurance to trust these applications from a third party that they already know and trust.

Using a password manager as a secure storage for other important data was the most important feature from the participants' point of view. In addition to login data, many people own other important data that they need to carry, such as their credit card details and Wi-Fi password. A password manager can be used as secure storage to safely record this important information for later use.

Among the emergency features provided by many password managers, master key recovery support technique was the most important feature. Users might be concerned about the possible scenario of forgetting the master key and not being able to access all of their recorded passwords in the password manager. Not many users see offline access to the password manager as an important feature. This might be because of the low rating of the cloud-based password manager, given that the offline access feature is only relevant for cloud-based services. The least important access support feature was to provide emergency access to other users. This could be due to confidentiality concerns.

Regarding the convenience features provided by the password managers, all of these features were highly rated: Synchronisation was the most important one, followed by the auto-filling feature then the method for fast access. This result illustrates a user's need to manage their credentials across different devices. Also, it emphasises the difficulties associated with typing passwords manually in to the smartphone. Furthermore, having a way to access the password manager without typing the master key is ranked as important. Users may need to apply this method sometimes when the risk of losing their device is low, for example: when they are at

home.

Unexpectedly, a free-of-cost password manager was not amongst the highly rated features, which suggests offering a password manager that provides the highly rated features with some cost.

Users' selected features while using the recommender system were recorded in a database. The frequencies of selecting each of the 13 features were consistent with users' reported rating of the importance of these features. The majority of the users were seeking an open source password manager, local-based password manager and/or a password manager that was developed by a well-known security company. These three features can be related to trust and privacy concerns. This suggests for password manager developers that developing security software such as anti-viruses and advertising them with the password manager can convince more potential users to choose their applications.

Although only 26% were looking for a password manager that provided functionality for safely sharing passwords with others, it is not clear whether the reason was that they did not share passwords, or that they preferred to share them using the traditional way. Further investigation is needed about supporting safe sharing of passwords using a password manager.

6.7 Conclusion

This chapter determined whether security interventions could encourage the adoption of a password manager by meeting people's self-determination needs. A longitudinal experiment was conducted, offering people a recommender application that met SDT needs, and their devices were monitored to see whether they subsequently installed a password manager. The recommender application convinced 139 participants to install a password manager on their device. The study discovered that satisfying autonomy and relatedness needs did indeed encourage adoption.

Chapter 7

Discussion and Implications

7.1 Introduction

This chapter reflects on the findings of this research, as reported in the previous chapters. The study's results are interpreted and recommendations suggested. Particularly, this chapter aims to bring together all the findings reported in this thesis. This begins with the findings of the exploratory study, which investigated the current status of password manager usage (Chapter 3). This is followed by the findings of the experimental and survey study, which investigated the factors influencing the intention to adopt a password manager (Chapter 5) and tested the effect of using recommendation applications that applied SDT factors (autonomy, relatedness and competence) on encouraging the adoption of a password manager (Chapter 6). This chapter concludes with some implications based on the findings for developers, service providers and scholars concerned with adopting security tools.

7.2 How Do Users Adopt a Password Manager?

As initially outlined (Chapter 2), contemporary literature offers considerable evidence for the persistence of the password problem and the potential benefits of using password managers for managing the password security and usability problem. The exploratory study reported in Chapter 3 showed that the adoption process consists of six stages: (1) awareness, (2) intention, (3) searching, (4) deciding, (5) trying and (6) long-term adoption (Figure 3.2). The study collected data from two sources (refer to section 3.2 and section 3.3 for more details): reviews from application stores of two popular password manager applications: LastPass and 1Password; and an online survey. The survey found that only 7% of the participants reported that they used a password manager on their smartphone devices; confirming the low adoption rate of these tools. Aiming to develop an exploratory theory from the qualitative data, Ground Theory methodology was used to analyse the data (section 3.4) starting from open coding, axial coding and selection coding to developing a theory. The study found that one of the main reasons for not

adopting password managers was the lack of awareness of the existence of these applications and it suggested using a proper awareness strategy for the password manager. Also, the study recommended that users needed to be supported in adopting password managers (section 3.6).

7.3 What Are the Factors That Inform Users' Intentions to Adopt a Password Manager?

After the users become aware of password managers, they will either intend to adopt one, or not. To understand the factors that influence the intention to adopt a password manager, two studies were conducted: an interview (section 5.3) then a survey (section 5.5.3). The analysis of the interviews resulted in the identification of factors that could be categorised as inhibitors or enablers when it comes to password manager adoption. The latter can be either push or pull factors. Accordingly, the migration model was used to model the adoption process and a password manager-switching model was developed and a set of hypothesis was proposed (section 5.4). A survey was designed (section 5.5.2) to test these hypotheses, and then quantitative data was collected from 198 Android smartphone users using a mobile application CyberPal (refer to section 5.5.3 for more details). Several analyses were conducted to evaluate the data validity (section 5.6.1). Then the proposed model was tested using the Structural Equation Modelling SEM approach (section 5.6.3 and section 5.6.4) and the hypotheses were tested. The quantitative analysis confirmed that users' dissatisfaction with their current coping behaviours pushes them away from these behaviours towards the intention to switch to the password manager. This dissatisfaction was found to be significantly influenced by users' perceived vulnerability to cyber security attacks and the cost of managing their passwords. The pull factors (the relative usefulness and the response efficacy of password managers) influence the intention to adopt password managers, while the mooring factors (set-up cost and users' perceived risk) deter intention to adopt password managers. The significant factors that influence the risk perception of password managers are security and privacy concerns. Moreover, descriptive norms have a positive effect on the intention to adopt a password manager (section 5.7).

7.4 The Need for Adoption Support

The exploratory study in Chapter 3 found that when the user intended to use a password manager they would need to search for a password manager and then decide whether it met their needs or not. If the password manager met their requirements, then they might install and try it. The experimental study in Chapter 6 showed that supporting users during the adoption process influences the adoption of password managers. The study tested the impact of using a recommendation application to support users during the searching and deciding stages of the password

manager adoption stages reported in Chapter 3. Also, it tested the impact of applying SDT's three factors in the recommendation application on the subsequent adoption process (section 6.2). Accordingly, two sets of hypotheses were formulated in section 6.2.1 and section 6.2.2. To test the first set of the proposed hypotheses, an intervention was designed and developed in the form of a smartphone recommendation application named CyberPal (section 6.3). Because awareness is the first stage of the adoption process (as reported in Chapter 3) and because of the lack of awareness of password managers, the recommendation application raised the awareness of these tools using an awareness video (section 6.3.1). The recommendation application (CyberPal) offers 13 options of requirements of the password manager. Based on the users' selected requirements, it suggests suitable password manager/s (section 6.3.2). The application basically supports the searching and decision stages of adopting a password manager. Furthermore, it monitors users' devices to see whether an installation was performed or not. The result of the experiment reported in section 6.5.1 showed that the recommendation application significantly encouraged users to install password managers on their devices. Reporting the intervention rate is recommended for information systems security studies [287]. In the case of CyberPal, the intervention rate is around 30%; which is a relatively effective rate compared to the reported adoption rate in previous studies [56], [30], [67] and [106].

Each tool or recommended behaviour has its own adoption process from the end users' point of view. For example, many users postponed their decision to update (patch) the operating system of their device by clicking "remind me later". Understanding the reason for any secure or insecure behaviour from the users' point of view is essential. This could be because of their fear of losing their data, such as contacts, photos or documents, which leads to them postponing the update until they find time to search for a solution to the potential loss problem. Integrating a message that gives options for backing up their data or ensuring that no data will be lost when asking them to update could influence more users to click on "update now", instead of relying on "remind me later".

7.5 The Power of SDT in Adopting Password Managers

Given the success of SDT in changing users' behaviour (Chapter 4), the SDT theory was used to meet users' autonomy, relatedness and competence needs in the recommendation intervention application. As reported in Chapter 6, the experiment also tested the impact of the different combinations of the SDT factors (autonomy, relatedness and competence) on encouraging the adoption of a password manager. Therefore, different strategies to support each of the three factors were identified from the literature (Table 6.1). These strategies were applied in the recommendation intervention CyberPal (section 6.3.2).

To test the second set of hypotheses reported in section 6.2.2, a factorial experiment was designed using different versions of the application CyberPal (section 6.4.1). Each version supported different combinations of the three factors of SDT. The experiment was conducted with 470 Android smartphone users (section 6.5) and it showed that autonomy and relatedness had a significant effect on the password manager adoption rate. The effect of competence, however, was not significant. Possible justification for this unexpected result is that competence might be less effective with critical systems. A critical system is the system, whose failure may cause catastrophic consequences, e.g. loss of life, significant property damage or environment. Bonini [284] 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 [285]. The study was a short-term experiment and, given the criticality of the data, it might be that more time is needed to develop a feeling of competence. Finally, electronic recommendations might create more uncertainty than face-to-face interaction with an expert [286], by exacerbating feelings of uncertainty; which in turn deter the competence.

7.6 Implications

The current research has resulted in some practical suggestions for developers, designers, service providers and security advisors to improve the adoption of password manager applications and other security behaviour. Also, some research implications are suggested for the benefit of scholars in the area of information security behaviours.

Research implications:

Generally, this research was a two-phase study. It first examined the determinants of password manager adoption using migration theory and secondly it explored the impact of SDT and recommendation system on adoption behaviours. Both studies have implications for future research in information security behaviour. The research contributes to the information security behaviour literature in several ways.

First, the comprehensive approach adopted in this research, where qualitative and quantitative data are used to deliver an enhanced view of the determinants of password manager adoption. Since each specific security behaviour has its own context of applicability, it is recommended that it be dealt with as a unique behaviour. There is a need to deal with each security behaviour independently and to understand the factors that may affect it from the users' point of view via qualitative studies.

Second, the research presents one of the first theory-based models of information security migration that can inform and guide future research in this area. The existing adoption model cannot readily be used to explain password manager migration because migration occurs from an incumbent coping behaviour triggering a substitute application, while adoption models do not acknowledge the presence of an incumbent status (current behaviour). At a time when the majority of end users already have their own coping strategies to deal with the password problem, the migration model is more worthy of a research investigation than the usual technology adoption models.

Furthermore, this study identified several factors influencing the intention to adopt password managers that are combinations of factors from both the incumbent status of the user, and their perceptions about password managers within the same framework.

Prior information security research applied theories from other disciplines such as health and justice. The research introduces migration theory as another useful theory for information security behavioural research, and, more generally, a theory from a new discipline (i.e. human geography), being used as a new reference theory to model information security research.

In addition, the research combines both inhibitors and enablers within the same theoretical model. It draws attention to the negative factors or barriers to the recommended security behaviour, such as switching costs and the perceived risk, which deter the migration intention.

Third, these findings of this research have important theoretical implications for SDT in the information security domain. Interventions that supported the three SDT factors predicted higher levels of password manager adoption, suggesting that supporting these needs is conducive to end users' adoption of password managers. Specifically, the research provides evidence of the importance of supporting autonomy and relatedness in information security behavioural change interventions. The competence factor needs more investigation to help understand the reasons for the insignificant effect of this factor in the study, given the importance of this factor in motivating humans in other life domains.

Finally, it is suggested that SDT be examined for studying a variety of information security behaviours, such as updating anti-viruses, applying email encryption, adopting anti-theft applications or backing up data.

Practical implications:

The research presented in this thesis has several practical implications.

The research found that a lack of awareness of password managers creates a critical barrier that prevents the successful adoption of these tools. Hence, it suggests that service vendors and security advisors consider password manager awareness as the first step in the adoption of these tools. They need to pay attention to awareness sessions as a means of encouraging password manager adoption. For instance, social media applications could be utilised to promote the utility of these applications.

The development of the recommendation system CyberPal can help smartphone users to by recommending a suitable password manager based on their requirements.

The findings indicated how supporting end users in the process of adopting password managers, through an intervention, can influence their adoption. Security advisors should exploit this advantage by providing appropriate support for each recommended behaviour.

Also, this study provides developers and service providers with a valuable reference about the socio-cultural impacts that influence the adoption of password manager applications. Because intention shapes users' behaviour towards the adoption of password managers, the pull, push and mooring factors are considered to be cornerstones for improving the adoption of these tools. Accordingly, these factors can be used in marketing and awareness campaigns to trigger and strengthen the intention to adopt a password manager.

The findings confirmed that social norms are one of the most significant channels in influencing the adoption of password managers. Thus, it is recommended that this channel be used to widely spread system awareness.

Furthermore, applying the SDT factors influenced the adoption of a password manager; thus, this theory should be exploited in security interventions to encourage the adoption of security tools and enhance the security behaviour of end users. In particular, supporting autonomy and relatedness through an intervention will provide greater opportunities for adopting the recommended security behaviour. For example, service providers can open 24/7 online communication with end users, to answer all their inquiries regarding any issue. Such a policy will enhance user satisfaction and increase confidence in the service provider.

7.7 Conclusion

This chapter discussed the findings from this research. It has linked the results of each study and justified the final findings. Further, it suggests some recommendations for password manager

developers, providers and researchers.

Chapter 8

Conclusion

This chapter provides a summary of the research and the key findings of this PhD research. It discusses the primary contributions of this research to the body of knowledge. Next, a discussion of the research limitations is provided. The chapter concludes with some suggestions for future research.

8.1 Thesis Summary

The primary goal of this research was to address the password problem for end users by encouraging the adoption of password managers. Managing passwords is exhausting for users, and coping skills weaken passwords, making them more vulnerable to attack. One of the available solutions to this problem is password manager applications. Yet, these tools are not yet widely adopted. In this thesis, the adoption of password manager applications has been investigated. The research explored the current state of password manager usage, identified the significant behavioural antecedents of adopting these tools and experimentally tested the impact of satisfying self-determination needs in an intervention encouraging the short-term adoption of password manager applications.

At the start of this research, a literature review was carried out to understand password issues and the efforts conducted towards addressing these issues (Chapter 2). It was concluded that current techniques do not solve the password problem. Moreover, the alternative approaches to the text-based password are not viable. Although password management systems seem a promising approach to address the password problem, the review found that most of the existing research only considered the issue from a technical prospective. There is an obvious lack of consideration of human aspects when adopting password managers.

A study was conducted to explore the current status of password manager adoption and issues with adopting these tools (Chapter 3). The study collected data from two sources to understand

the factors that impeded or encouraged the adoption of password managers. Grounded Theory was used to analyse the data and a theory of password manager adoption stages emerged from the data. It was revealed that the adoption process goes through six stages: (1) awareness, (2) intention, (3) searching, (4) deciding, (5) trying and (6) long-term adoption. The results suggested supporting users with a recommendation system that helps to search for and decide on a suitable password manager.

The factors that influence the intention to adopt a password manager were identified and empirically validated using a migration theoretical model (Chapter 5). These factors were identified based on interviews with smartphone users, resulting in a proposed migration mode. Then, the proposed model was tested quantitatively with smartphone users. The quantitative data was analysed using SEM. The study found that users' dissatisfaction with their password coping behaviours, and their perception of the usefulness and the effectiveness of password managers, influenced their intention to adopt a password manager. However, the perceived risks of using password managers, and the cost of setting up these tools, deterred the intention to adopt. Also, the result confirmed the positive influence of descriptive norms on adoption intention.

A smartphone intervention was designed and developed in the form of a password manager recommender system named "CyberPal". The app raised awareness of password managers and supported users in searching and deciding, then observed whether an initial trial ensued or not. Furthermore, the intervention was designed to support the three factors of SDT: autonomy, relatedness and competence. To test the impact of using a recommendation system, and the impact of applying the STD factors, a factorial experiment was conducted in the wild using nine versions of the intervention (Chapter 6). The study found that supporting users through a recommendation application significantly encouraged the adoption of these tools. Also, the study provided evidence that supporting the three basic needs in SDT, in particular autonomy and relatedness, is effective in encouraging the adoption of password managers.

8.2 Contributions

The present research makes several contributions that can be summarised in the following points:

First, identifying the password problem research gap. The literature review is provided to gain a better understanding of the state of the art of the password problem and the research effort made towards solving this problem. It has been found that extant proposed solutions and techniques do not solve the password problem. Moreover, there is an apparent lack of research considering the adoption of password management applications from a human perspective.

Second, identifying password manager adoption stages. A qualitative study was conducted to understand the factors that impeded or encouraged the adoption of password managers. The data was analysed using Grounded Theory, and it was found that the password manager adoption process goes through six stages. Accordingly, recommendations were suggested to improve the adoption of password manager applications.

Third, applying a migration theoretical model for adopting a password manager. An integrative framework of password manager migration was developed using migration theory as a theoretical foundation. It empirically validated the factors that influence or deter the intention to adopt a password manager application among smartphone users. The research draws attention to migration theory to demonstrate the migration from password coping behaviours to the use of password manager applications. It introduces migration theory as a referent theory that can be applied to understand other phenomena in information security tool adoption studies.

Fourth, designing an effective information security intervention. An intervention to encourage the adoption of a password manager was designed and experimentally validated. It was specifically designed as a recommendation system to support the adoption stages of a password manager from the users' point of view. It successfully convinced 30% of the participants to install a password manager; which is considered a relatively good effective intervention rate.

Fifth, applying SDT in an information security intervention. Uniquely, this research has applied SDT in an information security intervention. Using a 2*2*2 factorial experiment design method, the research provides evidence that supporting the three basic SDT needs, in particular autonomy and relatedness, is effective in encouraging the adoption of password managers; which suggests that applying a SDT intervention in information security domain was appropriate.

Finally, identifying the most preferred password manager features. The research also contributes to the body of password manager knowledge by identifying the end users' most preferred features of these applications. These findings can be used to inform future research to design a password manager application that more adequately satisfies end users' requirements and expectations.

8.3 Limitations

Like most research projects, there are some limitations to this research that have to be acknowledged.

Given that the experiment was conducted in the wild, participants paying attention to the language used by the recommender application was not ensured. Also, manipulation checks were not conducted to ensure that the variations in the intervention design had their intended effects. A FAQ feature was included to satisfy the competence need, but one cannot be sure that it actually did so. Nevertheless, according to O’Keefe [178], when message variations are identified in terms of intrinsic motivation, manipulation checks are unnecessary.

Another limitation in this research is in the use of a migration theoretical study. Due to the small sample size used to test the switching model, moderation analysis was not conducted to examine whether the relationships between the pull and push factors and the adoption intention were moderated by the mooring factors, or not. Furthermore, 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.

Sampling bias was another possible limitation in this research, since the study encouraged participants to recruit other participants in order to support the relatedness need, which may have led to a sampling bias. In addition, while the experiment 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.

Finally, it is worth mentioning that a recent study [289] investigated the security of four popular password manager services and found some vulnerabilities that can lead to hacking the data. For example, they found in 1password (Windows version) that the master password was stored in the memory in a plaintext format.

Nonetheless, despite the discovered problems, the researchers confirmed that password managers are still better than using the same simple, easy-to-crack passwords across many accounts.

8.4 Future Research Directions

The studies conducted in this research suggest some future research avenues.

The research discovered that satisfying the three needs of SDT in a password manager recommendation application, particularly autonomy and relatedness, did indeed encourage adoption of these tools. It determined whether or not the users had installed a password manager on their devices; which does not mean that they would continue using it in the long term. It would be interesting to monitor usage longitudinally and explore the factors that affect the long-term adoption of this tool. This might involve investigating the effect of poor design or design con-

straints of password manager and the features that are most preferred by participants, and which might encourage or discourage the long-term adoption of this tool. This is especially important giving that some users might have positive perception about password manager but do not use it.

Another direction for future work stemming from this research would be to focus more closely on meeting competence needs, to find ways of satisfying this need more effectively and to test its effect on encouraging the adoption of password manager applications.

More generally, this thesis suggests examining SDT when studying a variety of information security behaviours. For example, future research should apply SDT to encourage the adoption of other important security behaviours such as updating anti-viruses, applying email encryption, adopting anti-theft applications or backing up data.

Although most of password manager applications require strict requirement for the master key, there is no evidence from the literature that end-users are creating secure master keys for their password manager. More research is needed to explore whether the fact that password managers require users to memorise, only, one master password would lead to creating a strong master key and how to help users to adopt secure password behaviour for their master key.

In addition, this research found that the function to automatically change passwords was not rated, by participants, as an important feature of password manager. This suggests further research to understand the reason for this low rate

Furthermore, this thesis introduced migration theory as a new reference theory for model adoption in information security research. It would be interesting to use this theory in future research to study other switching security and privacy behaviours, for example, switching to security tokens such as "Yubikey" or switching from the "WhatsApp" communication application to other secure applications like "Telegram". This thesis suggests that using mixed methods to study and understand the recommended behaviour is essential. It stresses the importance of identifying the effective factors from qualitative data before verifying them quantitatively in order to find practical suggestions to support the behaviour of interest.

Appendix A

Online Survey

A.1 Survey Questionnaire

A Password Manager is software that remembers all your passwords for you, and can help to generate strong passwords for your logins. You only remember one master password to access all your passwords.

1. Do you use password manager in your computer?
2. Do you use password manager in your smartphone?
If yes in (2):
3. Which password manager application do you use in your phone?
4. What do you like about this password manager application?
5. What makes you use a password manager application on your smartphone?
If No in (2):
3. Why do you choose not to use a password manager application?
4. What would make it possible or easy for you to start using a password manager application on your smartphone?

A.2 Participant Consent Form

Dear Participant,

This survey seeks to understand Smartphone users perspective about using Password Manager applications as part of my PhD research in Glasgow University under the supervision of Dr.Karen Renaud.

I will anonymise any responses you provide and ensure that no one is identifiable from anything I publish as an outcome of this survey. Please do not tell me anything about your actual passwords or any information that might constitute a hint to one of your own passwords.

You are free to withdraw from this survey at any time.

Please check the box to confirm that you are over 18 ☐

Please check this box to agree to take part in this research ☐

Here is my email address in case you wish to contact me about this survey:

n.alkaldi.1@research.gla.ac.uk

Many thanks for participating.

Nora Alkaldi

A.3 Ethical Approval

1



Institute of Neuroscience
and Psychology

Dr. Peter J. Uhlhaas
Reader

Chair, College Ethics Committee

58 Hillhead Street, University of
Glasgow, Glasgow, G12 8QB,
Scotland
tel: +44 (0) 141 330 8730
email: peter.uhlhaas@glasgow.ac.uk

10th of April 2016

Ethics Application No: 300150084

Dear Dr Renaud,

this is to let you know that your submission “password manager applications” has been approved by the Ethics Committee of the College of Science and Engineering.

Sincerely yours,

Peter Uhlhaas

Appendix B

Interview Study

B.1 Questionnaire Script

B.1.1 Demographic Data

Q1. Age: What is your age?

18-24 years old

25-34 years old

35-44 years old

45-54 years old

55-64 years old

65-74 years old

75 years or older

Q2. Gender: What is your gender? (Male / Female)

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

No schooling completed

Nursery school to 8th grade

Some high school, no diploma

High school graduate, diploma or the equivalent (for example: GED)

Some college credit, no degree

Trade/technical/vocational training

Associate degree

Bachelor's degree

Master's degree

Professional degree

Doctorate degree

B.1.2 Smartphone Usage and Password Experience

Q1. What is your smartphone operating system?

Apple iOS

Android

Windows phone

Blackberry

Others (please specify)

I don't know

Q2. Do you use screen lock mechanism in your smartphone(e.g. PIN and fingerprint)?

(Yes/ No)

If yes in Q2:

What type of locking mechanism do you use on your smartphone?

Numerical password (PIN)

Alphanumeric password (characters and/or numbers)

Graphical password (patterns)

Fingerprint, Facial recognition

Other(please specify)

Why do you prefer this particular locking mechanism?

If No in Q2:

Why do not you think you need a locking mechanism?

Q3. On a typical day, how many passwords do you enter in your smartphone?

None

Up to 3

4 or 5

6 or 7

8 to 10

More than 10

Q4. Have you ever bought anything via your smartphone?

Yes, via app

Yes, via web

No

Q5. How do you manage your passwords?

Q6. Do you ever use the same password for two or more accounts? (Yes/ No)

If yes in Q6:

Why do you think people use the same password for two or more accounts?

Q7. How many times did you use password recovery/reset mechanisms in the last 6 months

(e.g. use forget my password function)?

Q8. Do you write down your password somewhere? (Yes/No)

Q9. Do you save your password in the web browser in your device (ie: when you access your account in a website it automatically fills in your authentication details? (Yes/ No)

B.1.3 Password Manager

Password manger is software that store and organizes passwords securely. It automatically fills in your passwords for you. Most of them require one strong password or a finger print.

Examples: LastPass, 1Password,Dashlane

Q1. Do you use a Password Manger? (Yes/No)

If Yes in Q1:

What the password manger do you currently use?

Why did you choose this particular password manager?

Q2. What do you think the advantages would be of using a password manager application in your smartphone?

Q3. What do you think the disadvantages would be of using a password manager application in your smartphone?

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

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

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

Q7. Who do you take security advice from?

If No in Q1:

Q8. Is there any thing specific that prevent you from using a password manager in your phone?

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

If Yes in Q1:

Q8. Do you think there is any difficulties or barriers to use password manager applications in the phone?

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

B.2 Participant Consent Form

Understanding SmartPhone users' beliefs about Password Managers

Dear Participant,

This survey seeks to understand the beliefs of Smartphone users about Password Manager applications.

I will anonymise any responses you provide and ensure that no one is identifiable from anything I publish as an outcome of this research. Please do not tell me anything about your actual passwords or any information that might constitute a hint to one of your own passwords.

You are free to withdraw from this survey at any time.

Many thanks for participating in my research project

Check this box to agree to take part in this survey ☐

Here is my email address in case you wish to contact me about this survey:

n.alkaldi.1@research.gla.ac.uk

B.3 Ethical Approval

1



Institute of Neuroscience
and Psychology

Dr. Peter J. Uhlhaas
Reader

Chair, College Ethics Committee

58 Hillhead Street, University of
Glasgow, Glasgow, G12 8QB,
Scotland
tel: +44 (0) 141 330 8730
email: peter.uhlhaas@glasgow.ac.uk

13rd of February 2016

Ethics Application No: 300150074

Dear Dr Renaud,

this is to let you know that your submission "Password Manager Applications" has been approved by the Ethics Committee of the College of Science and Engineering.

Sincerely yours,

Peter Uhlhaas

Appendix C

Experiment

C.1 Password Manager Features

password manager name	cloud storage	local storage	open source	Free	security Company	Sync.	2 Fact Auth	Export passwords	Fast Access	Master Key Recovery Support	Share Passwords	Location Access Restriction	Security Feedback	Track Activities
KeePass2Android		X	X	X		X	X	X	X					
PasswdSafe		X	X	X		X	X	X			X			
Bitwarden	X		X	X		X	X	X	X	X	X			
keepassDroid		X	X	X		X	X	X						
LastPass	X			X		X	X	X	X	X	X	X	X	X
Enpass		X				X		X	X		X			
DashLane	X			X			X	X	X	X	X		X	
KasperSky	X				X	X		X	X				X	
Padlock		X	X	X				X						
Zoho	X			X		X	X	X	X				X	X
Norton	X			X	X	X	X	X	X	X				
Roboform	X					X	X	X	X	X	X		X	X
1Password	X					X	X	X	X	X	X		X	
TrueKey	X			X	X	X	X	X	X	X				
Keeper	X					X	X	X	X	X	X		X	X
Encryptr	X		X	X		X								
Zoho Pro	X					X	X	X	X		X	X	X	X
DashLane Pro	X					X	X	X	X	X	X		X	
Padlock Premium	X		X			X		X						

C.2 Pre questionnaire

Q1. Gender: What is your gender?

- A Male
- B Female
- C Prefer not to answer

Q2. Age: What is your age group?

- A 18-25
- B 26-35
- C 36-45
- D 46-55
- E 56-65
- F 66-75
- G 75+
- H Prefer not to answer

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

- A Less than a high school diploma
- B High school degree or equivalent (e.g. GED)
- C Some college, no degree
- D Associate degree (e.g. AA, AS)
- E Bachelor's degree (e.g. BA, BS)
- F Master's degree (e.g. MA, MS, MEd)
- G Professional degree (e.g. MD, DDS, DVM)
- H Doctorate (e.g. PhD, EdD)
- I Other: (please specify)

Q4. How many passwords do you currently have?

- ☐ <3, ☐ 3-5, ☐ 6-9, ☐ 10-15, ☐ 16-20, ☐ 21-25, ☐ Over 26

Q5. How would you rate your Information Security knowledge on the following scale?

Very low  Very High

Q6 : How would you rate your Internet/computer skills?

Novice  Expert

Q7. Did you know about password managers before using CyberPal?

- ☐ Yes, ☐ No

If Yes in Q7:

From the following apps, select only two popular password manager applications:

- A DashLane
- B CM Locker
- C LastPass
- D Screen Off and Lock
- E Keypad Lock Screen

Do you use a password manager?

☐ Yes, ☐ No

If Yes:

On which devices do you use it?

☐ Mobile device ☐ Computer ☐ Both

Q8. How do you manage your passwords? (Please, select all applicable answers)

- A My browser remembers my passwords for me
- B I write my passwords in a notebook
- C I use the same password to access multiple accounts.
- D I use similar passwords by slightly modifying a password
- E I use personal information such as a pet's name or date of birth
- F I use other applications e.g. Google authenticator
- G Others (please specify)

Q9. Please give yes or no answers for the following questions about hacking experience; if your answer is "yes" please indicate the degree to which that experience affected you (in terms of lost data, lost time, monetary losses, identity theft etc.)

1. Have you ever had an important email account a social networking account an online shopping account or online banking account hacked?

☐ Yes, ☐ No

If yes: Please indicate the degree to which that experience affected you (in terms of lost data, lost time, monetary losses, identity theft etc.)

Low impact  High impact




2. Has someone you know personally ever had their important email account, social network account, online shopping account or online banking account, hacked into?(Yes, No).

☐ Yes, ☐ No

If yes: Please indicate the degree to which that experience affected you (in terms of lost data, lost time, monetary losses, identity theft etc.)

Low impact  High impact








Q 10. Rate the following statements:













1. I intend to use a password manager within a week.
Strongly Disagree  Strongly Agree
2. I predict I will use a password manager within a week.
Strongly Disagree  Strongly Agree
3. I plan to use a password manager within a week.
Strongly Disagree  Strongly Agree





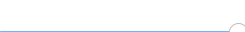








(If 'No' is selected in Q7 the rest of the questions are skipped)













(To minimize position bias, items were jumbled up rather than logically grouped)

Q11. Rate the following statements considering your current method for managing your passwords and your opinion about using password managers. If you are already using a password manager, consider the scenario before you start using the password manager:

1. Most of my friends are using a Password Manager.
Strongly Disagree  Strongly Agree
2. Most of my family members are using a Password Manager.
Strongly Disagree  Strongly Agree
3. Most of my co-workers are using a Password Manager.
Strongly Disagree  Strongly Agree
4. Most people I know are using a Password Manager.
Strongly Disagree  Strongly Agree
5. Other people come to you for advice on new technologies.
Strongly Disagree  Strongly Agree
6. In general, you are among the first in your circle of friends to acquire new technology when it appears.
Strongly Disagree  Strongly Agree
7. You can usually figure out new high-tech products and services without help from others.
Strongly Disagree  Strongly Agree

8. Managing my passwords currently requires a considerable investment in Time.
Strongly Disagree  Strongly Agree
9. Currently, there are too many overheads associated with Managing my passwords.
Strongly Disagree  Strongly Agree
10. Managing my passwords currently requires a considerable effort other than time.
Strongly Disagree  Strongly Agree
11. Managing my passwords currently causes problems such as memorability issues and task delay.
Strongly Disagree  Strongly Agree
12. There is a chance that someone could successfully guess at least one of my passwords.
Strongly Disagree  Strongly Agree
13. There is a chance that someone could successfully crack at least one of my passwords using password cracking software.
Strongly Disagree  Strongly Agree
14. There is a chance that someone could hack into at least one of my important email accounts.
Strongly Disagree  Strongly Agree
15. If someone hacked into my important email account there is a chance that they could guess my other important passwords.
Strongly Disagree  Strongly Agree
16. How do you feel about your overall experience with the current method for managing your passwords:
Extremely Dissatisfied  Extremely Satisfied
17. How do you feel about your overall experience with the current method for managing your passwords:
Extremely Unpleasant  Extremely Pleasant
18. How do you feel about your overall experience with the current method for managing your passwords:
Extremely Terrible  Extremely Delightful
19. The fee that I have to pay for the use of a password manager would be too high
Strongly Disagree  Strongly Agree

20. The fee that I have to pay for the use of a password manager would be reasonable
Strongly Disagree  Strongly Agree
21. I would be pleased with the fee that I have to pay for the use of a password manager
Strongly Disagree  Strongly Agree
22. It will take me a lot of time to learn to use a Password Manager's features.
Strongly Disagree  Strongly Agree
23. It will take me a lot of effort to get up to speed and use a Password Manager.
Strongly Disagree  Strongly Agree
24. Learning to use a Password Manager well will be difficult.
Strongly Disagree  Strongly Agree
25. It will take a lot of time to set up my device and online accounts to use a Password Manager
Strongly Disagree  Strongly Agree
26. It will take a lot of effort to set up my device and online accounts to use a Password Manager.
Strongly Disagree  Strongly Agree
27. Overall, the process involved in setting up a Password Manager is very elaborate.
Strongly Disagree  Strongly Agree
28. Using a password manager leads to a loss of control over the privacy of my passwords and personal data.
Strongly Disagree  Strongly Agree
29. Using a password manager allows others to view my passwords and personal data.
Strongly Disagree  Strongly Agree
30. Overall I see a privacy threat linked to password manager's usage.
Strongly Disagree  Strongly Agree
31. Password managers implement security measures to protect my passwords from being hacked
Strongly Disagree  Strongly Agree
32. Password managers usually ensure that transferring information is protected from hacking attacks
Strongly Disagree  Strongly Agree

33. I feel safe in saving my passwords on password managers
Strongly Disagree  Strongly Agree
34. I feel secure in managing my passwords using password managers
Strongly Disagree  Strongly Agree
35. Providing password manager with my passwords would involve many unexpected problems.
Strongly Disagree  Strongly Agree
36. It would be risky to put my passwords in a password manager.
Strongly Disagree  Strongly Agree
37. There would be high potential for loss in saving my passwords in a password manager.
Strongly Disagree  Strongly Agree
38. Password manager application works for protecting my passwords from being stolen and abused by attackers.
Strongly Disagree  Strongly Agree
39. Password manager application is effective solution for protecting my passwords from being stolen and abused by attackers.
Strongly Disagree  Strongly Agree
40. When using a password manager application, my passwords are more likely to be protected from being stolen and abused by attackers
Strongly Disagree  Strongly Agree
41. Using a Password Manager will help me accomplish my tasks more quickly than my current method for managing my passwords.
Strongly Disagree  Strongly Agree
42. Using a Password Manager will improve my performance as compared to my current method for managing my passwords.
Strongly Disagree  Strongly Agree
43. Using a Password Manager will enhance my effectiveness more than my current method for managing my passwords.
Strongly Disagree  Strongly Agree
44. I will find using a Password Manager to be more useful than my current method for managing my passwords.
Strongly Disagree  Strongly Agree

C.3 Post questionnaire

Q1. Have you installed a password manager?

- A No
- B Yes, installed it but I have not used it yet.
- C Yes, installed and used a password manager.
- D I am already using a password manager before using CyberPal app.

If B,C or D:

Q2. What are the main reasons for you to install a password manager on your smartphone?

(Please, select all applicable answers)

- A To support my own memory (i.e. I can't remember all my passwords)
- B To use the auto-filling feature of user name and password when I login to my accounts
- C To keep my passwords synchronized across all my devices
- D To have a safe way to share some of my passwords
- E To improve the security of my passwords e.g use system generated passwords /use unique passwords for each of my accounts
- F To have a secure storage for important data such as credit card details
- G Other reason (Please specify)

If A:

Q2.Why did you decide not to install a password manager on your Smartphone?

(Please, select all applicable answers)

- A Because of phone related issues (i.e. Insufficient memory space, the device is slow or the battery is consumed quickly)
- B Because it takes time to set up a PM.
- C Because I don't trust my phone device to be free of viruses or malware. (e.g. hackers can spy on my phone and steal my passwords or compromise the PM)
- D Because my phone could get lost/stolen at any time
- E Because I don't trust PM applications, even if my friends or family members use them.
- F Because I don't want to be the first one in my family and friends to use a PM application.
- G Because I can't decide which PM application to use
- H Because I don't know how to use a PM application
- I Because I don't need a PM application
- J Other reason (please specify)

Q3. For password manager applications, rate the following features from 1 to 5, 1 being the least important and 5 being the most important feature:

1. Provides a secure storage for other types of data such as Wi-Fi passwords, notes or images.
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
2. Synchronising passwords across devices.
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
3. Provides communication channel for customer support (e.g. live chat)
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
4. Exports passwords for safe keeping
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
5. The source code is open and available to everyone.
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
6. Developed by a well known security application provider such as McAfee.
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐
7. Stores passwords locally on the device only (not on the cloud).
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
8. Allows user to clear out all passwords and other data.
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
9. Provides feedback to assist the security of all passwords (e.g. percentage of passwords uniqueness or their strength).
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
10. Supports two factor authentication.
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
11. Restricts access to certain geographical locations (e.g. allow access only from a specific country).
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
12. Provides a quick and easy-access option to the password manager (e.g. fingerprint or PIN code).
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
13. Has social network accounts to be updated with the latest news and to communicate with other password manager users.
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
14. Allows users to set up an automatic logout timer.
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

15. Imports passwords from browsers /other password managers.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

16. Supports master key recovery (e.g. Hint).

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

17. Stores passwords on the cloud.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

18. Auto-fills login forms on websites.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

19. Supports offline access to the password manager.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

20. The password manager is free of charge.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

21. Safely shares passwords with family members/collaborators.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

22. Changes passwords automatically for you.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

23. Tracks and records activities in the password manager (e.g. timestamp of when a password was used).

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

24. Allows emergency access to trusted users.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

25. Provides pronounceable system generated passwords.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

26. Provides random system generated passwords.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

C.4 Participant Consent Form

This information was incorporated into the application

University of Glasgow, College of Science and Engineering Research Ethics Committee

The aim of this research is to examine whether smartphone users will install and use password manager application when they become aware of it through recommender mobile application CyberPal. Also, the research aims to examine the factors that can predict the intention or the usage of password manager applications.

I understand that the researcher is collecting data in the form of: completed questionnaires, the data I have submitted to the application including my phone number and the phone number of the person who tell me about this application, which buttons or choices I have click on or choose and when, my phone contact list, the name of other applications I have installed/uninstalled and the recently opened applications for use in an academic research project at the University of Glasgow.

I also understand that any other user of this application could see the name of the password manager application that I have in my device (if there is any).

Note that all data will be treated as confidential and kept secure at all times. The data will be retained in secure storage for use in future academic research. The data may be used in future publications, both print and online.

You can withdraw participation in the experiment at any time by e-mailing:
n.alkaldi.1@research.gla.ac.uk

☐ I declare that I am 18 or over years old

By clicking 'I Agree' you are providing consent.

Researcher's name and email contact:

Nora Alkaldi

n.alkaldi.1@research.gla.ac.uk

C.5 Ethical Approval



Dr. Christoph Scheepers
Senior Lecturer

School of Psychology
University of Glasgow
58 Hillhead Street
Glasgow G12 8QB
Tel.: +44 141 330 3606
Christoph.Scheepers@glasgow.ac.uk

Glasgow, June 7, 2017

Ethical approval for:

Application Number: 300160170

Project Title: Toward adopting password manager application among smartphone users
(Minor changes in application: 300160024)

Lead Researcher: Dr Karen Renaud

This is to confirm that the above application has been reviewed by the College of Science and Engineering Ethics Committee and **approved**. Please refer to the collated reviewer comments on the system for additional comments, if any. Good luck with your research.

Sincerely,

Dr Christoph Scheepers

Dr Christoph Scheepers
Ethics Officer
College of Science and Engineering
University of Glasgow

Bibliography

- [1] Adams, A., and Sasse, M.A. (1999). *Users are not the enemy* In: Communications of the ACM 42.12 , pp. 40-46.
- [2] Hoonakker,P., Bornoe,N., and Carayon,P. (2009). *Password authentication from a human factors perspective: Results of a survey among end-users* In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting 53.6 , pp. 459-463.
- [3] Zezschwitz, E.V., De Luca, A., and Hussmann, H., (2014). *Honey, I shrunk the keys: influences of mobile devices on password composition and authentication performance* In: Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational. ACM. , pp. 461-470.
- [4] Silver, D., Jana, S., Boneh, D., Chen, E. and Jackson, C., (2014). *Password managers: Attacks and defenses* In: 23rd USENIX Security Symposium (USENIX Security 14). pp. 449-464.
- [5] Al-Sinani, H.S. and Mitchell, C.J., (2010), November. *Using CardSpace as a password manager* In IFIP Working Conference on Policies and Research in Identity Management (pp. 18-30). Springer, Berlin, Heidelberg.
- [6] Stobert, E. and Biddle, R., (2014). *The password life cycle: user behaviour in managing passwords*. In 10th Symposium On Usable Privacy and Security (SOUPS 2014) (pp. 243-255).
- [7] Das, A. and Khan, H.U., (2016). *Security behaviors of smartphone users* Information & Computer Security, 24(1), pp.116-134.
- [8] Alshammari, N.O., Mylonas, A., Sedky, M., Champion, J. and Bauer, C., (2015), August. *Exploring the adoption of physical security controls in smartphones*. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 287-298). Springer, Cham.
- [9] Mylonas, A., Kastania, A. and Gritzalis, D., (2013). *Delegate the smartphone user? Security awareness in smartphone platforms*. Computers & Security, 34, pp.47-66.

- [10] Furnell, S., (2005). *Why users cannot use security*. In: Computers & Security 24.4 , pp. 274-279.
- [11] Prata, W., de Moraes, A. and Quaresma, M., (2012). *User's demography and expectation regarding search, purchase and evaluation in mobile application store*. In: Work, 41(Supplement 1), pp.1124-1131.
- [12] Sweeney, J.C., Webb, D., Mazzarol, T. and Soutar, G.N., (2014). *Self-determination theory and word of mouth about energy-saving behaviors: an online experiment*. In: Psychology & Marketing, 31(9), pp.698-716.
- [13] Sheldon, K.M., Elliot, A.J., Kim, Y. and Kasser, T., (2001). *What is satisfying about satisfying events? Testing 10 candidate psychological needs*. In: Journal of personality and social psychology, 80(2), p.325.
- [14] Fathali, S. and Okada, T., (2017). *A self-determination theory approach to technology-enhanced out-of-class language learning intention: A case of Japanese EFL learners*. In: International Journal of Research Studies in Language Learning, 6(4), pp.53-64.
- [15] Deci, E.L., (1972). *Intrinsic motivation, extrinsic reinforcement, and inequity*. In: Journal of personality and social psychology, 22(1), p.113.
- [16] Hsu, C.L., Wang, C.F. and Lin, J.C.C., (2011). *Investigating customer adoption behaviours in mobile financial services*. In: International Journal of Mobile Communications, 9(5), pp.477-494.
- [17] Ng, B.Y., Kankanhalli, A. and Xu, Y.C., (2009). *Studying users' computer security behavior: A health belief perspective*. In: Decision Support Systems, 46(4), pp.815-825.
- [18] Van Bruggen, D., Liu, S., Kajzer, M., Striegel, A., Crowell, C.R. and D'Arcy, J., (2013), July. *Modifying smartphone user locking behavior*. In: Proceedings of the Ninth Symposium on Usable Privacy and Security (p. 10). ACM.
- [19] Lee, E.S., (1966). *A theory of migration*. In: Demography, 3(1), pp.47-57.
- [20] Furnell, S., (2007). *An assessment of website password practices*. In: Computers & Security, 26(7-8), pp.445-451.
- [21] Antypas, K. and Wangberg, S.C., (2014). *Combining users' needs with health behavior models in designing an internet-and mobile-based intervention for physical activity in cardiac rehabilitation*. In: JMIR research protocols, 3(1).
- [22] Morris, R. and Thompson, K., (1979). *Password security: A case history*. Communications of the ACM, 22(11), pp.594-597.

- [23] Klatzky, R.L., (1975). *Human memory: Structures and processes*. New York: Freeman.
- [24] Miller, G.A., (1956). *The magical number seven plus or minus two: Some limits on our capacity for processing information*. Psychological Review, 63, 81-97.
- [25] Szmalec, A., Brysbaert, M. and Duyck, W., (2012). *Working memory and (second) language processing*. In Memory, language, and bilingualism: Theoretical and applied approaches (pp. 74-94). Cambridge University Press.
- [26] Woods, N., (2016). *Improving the security of multiple passwords through a greater understanding of the human memory*. Jyväskylä studies in computing, 249, 151 p
- [27] Cormac Herley, (2009). *So long, and no thanks for the externalities: the rational rejection of security advice by users*. In: Proceedings of the 2009 workshop on New security paradigms workshop. ACM. 2009, pp. 133-144.
- [28] Adam Beaument and Angela Sasse, (2009). *The economics of user effort in information security*. In: Computer Fraud & Security 2009.10 (2009), pp. 8-12.
- [29] Albrechtsen, E. and Hovden, J., (2009). *The information security digital divide between information security managers and users*. Computers & Security, 28(6), pp.476-490.
- [30] Wash, R., Rader, E., Berman, R. and Wellmer, Z., (2016). *Understanding password choices: How frequently entered passwords are re-used across websites*. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) (pp. 175-188).
- [31] Rinn, C., Summers, K., Rhodes, E., Virothaisakun, J. and Chisnell, D., (2015). *Password creation strategies across high-and low-literacy web users*. Proceedings of the Association for Information Science and Technology, 52(1), pp.1-9.
- [32] Zadorozhnyy, A., (2017). *The Impact of Social Networking Sites on English Language Learning* (Doctoral dissertation, Nazarbayev University Graduate School of Education).
- [33] Xu, Z., Wang, H. and Jajodia, S., (2014), October. *Gemini: An Emergency Line of Defense against Phishing Attacks*. In Reliable Distributed Systems (SRDS), 2014 IEEE 33rd International Symposium on (pp. 11-20). IEEE.
- [34] Loutfi, I. and Jäysang, A., (2015), February. *Passwords are not always stronger on the other side of the fence*. In Proc. Workshop on Usable Security (USEC). Internet Society, San Diego, CA, USA, 1-10.
- [35] Hayashi, E. and Hong, J., (2011). *A diary study of password usage in daily life*. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2627-2630). ACM.

- [36] Florencio, D. and Herley, C., (2007). *A large-scale study of web password habits*. In Proceedings of the 16th international conference on World Wide Web (pp. 657-666). ACM.
- [37] SANS, (2017). *Password Construction Guidelines* <https://www.sans.org/security-resources/policies/general/pdf/password-construction-guidelines> [Accessed January 10, 2017].
- [38] O’Gorman, L., (2003). *Comparing passwords, tokens, and biometrics for user authentication*. Proceedings of the IEEE, 91(12), pp.2021-2040.
- [39] Shen, C., Yu, T., Xu, H., Yang, G. and Guan, X., (2016). *User practice in password security: An empirical study of real-life passwords in the wild*. Computers & Security, 61, pp.130-141.
- [40] Greene, K.K. and Choong, Y.Y., (2017). *Must I, can I? I don’t understand your ambiguous password rules*. Information & Computer Security, 25(1), pp.80-99.
- [41] Han, G., Yu, Y., Li, X., Chen, K. and Li, H., (2017). *Characterizing the semantics of passwords: The role of Pinyin for Chinese Netizens*. Computer Standards & Interfaces, 54, pp.20-28.
- [42] Furnell, S. and Esmail, R., (2017) *Evaluating the effect of guidance and feedback upon password compliance*. Computer Fraud & Security 2017.1 : 5-10.
- [43] Egelman, S., Bonneau, J., Chiasson, S., Dittrich, D. and Schechter, S., (2012). *It’s Not Stealing If You Need It: A Panel on the Ethics of Performing Research Using Public Data of Illicit Origin*. In International Conference on Financial Cryptography and Data Security , Kralendijk, Bonaire, (Vol. 7398, pp 124-132). Springer.
- [44] Thomas, D.R., Pastrana, S., Hutchings, A., Clayton, R. and Beresford, A.R., (2017). *Ethical issues in research using datasets of illicit origin*. In Proceedings of the 2017 Internet Measurement Conference (IMC ’17). ACM, New York, NY, USA, (pp. 445-462). ACM.
- [45] Weir, M., Aggarwal, S., Collins, M. and Stern, H., (2010). *Testing metrics for password creation policies by attacking large sets of revealed passwords*. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 162-175). ACM.
- [46] Bonneau, J., Preibusch, S. and Anderson, R., (2012). *A birthday present every eleven wallets? The security of customer-chosen banking PINs*. In International Conference on Financial Cryptography and Data Security (pp. 25-40). Springer, Berlin, Heidelberg.
- [47] Yu, X. and Liao, Q., (2016). *User password repetitive patterns analysis and visualization*. Information & Computer Security, 24(1), pp.93-115.

- [48] Liu, Zhipeng, Yefan Hong, and Dechang Pi.(2014). *A Large-Scale Study of Web Password Habits of Chinese Network Users*. JSW 9.2 : 293-297.
- [49] Barbosa, N.M., Hayes, J. and Wang, Y., (2016). *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 (pp. 49-60). ACM.
- [50] Ahuja, R., Ramrakhyani, M., Manchundiya, B. and Shroff, S., (2016). *Dual Layer Secured Password Manager using Blowfish and LSB*. International Journal of Computer Applications, 143(3).
- [51] Bajpai, N., (2011). *Business research methods*. Pearson Education India.
- [52] Wang, L., Li, Y. and Sun, K., (2016). *Amnesia: A Bilateral Generative Password Manager*. In Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on (pp. 313-322). IEEE.
- [53] Bosnjak, L. and Brumen, B., (2016). *What do students do with their assigned default passwords?*. In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016 39th International Convention on (pp. 1430-1435). IEEE.
- [54] Taneski, Viktor, Marjan Hericko, and BoÅatjan Brumen.(2016) *Analysing real students' passwords and students' passwords characteristics received from a questionnaire*. Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016 39th International Convention on. IEEE, 2016.
- [55] Tullis, T.S. and Tedesco, D.P., (2005). *Using personal photos as pictorial passwords*. In CHI'05 extended abstracts on Human factors in computing systems (pp. 1841-1844). ACM.
- [56] Ur, B., Noma, F., Bees, J., Segreti, S.M., Shay, R., Bauer, L., Christin, N. and Cranor, L.F., (2015). *"I Added"! at the End to Make It Secure" : Observing Password Creation in the Lab*. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (pp. 123-140).
- [57] Melicher, W., Kurilova, D., Segreti, S.M., Kalvani, P., Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L.F. and Mazurek, M.L., (2016). *Usability and security of text passwords on mobile devices*. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 527-539). ACM.
- [58] Hancock, M., Calderon, F., Drayton, M., Stapleton, E., Nida, J., Williamson, S., Easter, A., Knight, S., Vazquez, A., Wade, R. and Woolfolk, D., (2016). *Multi-cultural Empirical*

- Study of Password Strength Versus Ergonomic Utility*. In *Advances in Human Factors in Cybersecurity* (pp. 315-326). Springer, Cham.
- [59] Lo, C.C.W., (2016). *Empirical Study of Secure Password Creation Habit*. In *International Conference on Augmented Cognition* (pp. 189-197). Springer, Cham.
- [60] Grawemeyer, B. and Johnson, H., (2011). *Using and managing multiple passwords: A week to a view*. *Interacting with Computers*, 23(3), pp.256-267.
- [61] Shay, R., Komanduri, S., Durity, A.L., Huh, P.S., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N. and Cranor, L.F., (2014). *Can long passwords be secure and usable?*. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2927-2936). ACM.
- [62] Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. and Cranor, L.F., (2010). *Encountering stronger password requirements: user attitudes and behaviors*. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 2). ACM.
- [63] Gerber, N. and Zimmermann, V., (2017). *Security vs. privacy? User preferences regarding text passwords and biometric authentication*. *Mensch und Computer 2017-Workshopband*.
- [64] Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N. and Cranor, L.F., (2016) . *Do Users' Perceptions of Password Security Match Reality?*. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 3748-3760). ACM
- [65] Farcasin, M. and Chan-tin, E., (2015). *Why we hate IT: two surveys on pre-generated and expiring passwords in an academic setting*. *Security and Communication Networks*, 8(13), pp.2361-2373.
- [66] Shay, R., Komanduri, S., Durity, A.L., Huh, P.S., Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N. and Cranor, L.F., (2016). *Designing password policies for strength and usability*. *ACM Transactions on Information and System Security (TISSEC)*, 18(4), p.13.
- [67] Zhang-Kennedy, L., Chiasson, S. and Biddle, R., (2013). *Password advice shouldn't be boring: Visualizing password guessing attacks*. In *2013 APWG eCrime Researchers Summit* (pp. 1-11). IEEE.
- [68] Choong, Yee-Yin, and Mary Theofanos.(2015) *What 4,500+ people can tell you-employees' attitudes toward organizational password policy do matter*. *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, Cham, 2015.

- [69] Fredericks, Damian Todd, Lynn Ann Fitcher, and Kerry-Lynn Thomson.(2016) *Comparing Student Password Knowledge and Behaviour: A Case Study*. HAISA. 2016.
- [70] Ives, B., Walsh, K.R. and Schneider, H., (2004). The Domino Effect of Password Reuse. COMMUNICATIONS OF THE ACM, 47(4), p.75.
- [71] Boothroyd, V. and Chiasson, S., (2013). *Writing down your password: Does it help?*. In Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on (pp. 267-274). IEEE.
- [72] Schneier,B. *Write Down Your Password*. http://www.schneier.com/blog/archives/2005/06/write_down_your.html, (June 2005). [Accessed January 10, 2017].
- [73] Petrie, Helen, and Burak Merdenyan. *Cultural and Gender Differences in Password Behaviors: Evidence from China, Turkey and the UK*.(2016) Proceedings of the 9th Nordic Conference on Human-Computer Interaction. ACM, 2016.
- [74] Whitty, M., Doodson, J., Creese, S. and Hodges, D., (2015). *Individual differences in cyber security behaviors: an examination of who is sharing passwords*. Cyberpsychology, Behavior, and Social Networking, 18(1), pp.3-7.
- [75] Lenhart, A., Duggan, M., and Smith A. (2014). *Couples, the Internet, and social media: How American couples use digital technology to manage life, logistics, and emotional intimacy within their relationships*. Pew Research Centre. Retrieved from <http://www.pewInternet.org> [Accessed January 10, 2017].
- [76] Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G. and Furlong, M., (2007). *Password sharing: implications for security design based on social practice*. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 895-904). ACM.
- [77] Meter, D.J. and Bauman, S., (2015). *When sharing is a bad idea: The effects of online social network engagement and sharing passwords with friends on cyberbullying involvement*. Cyberpsychology, Behavior, and Social Networking, 18(8), pp.437-442.
- [78] Kaye, J.J., (2011). *Self-reported password sharing strategies*. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2619-2622). ACM.
- [79] MATT RICHTER, (2012). *Young, in Love and Sharing Everything, Including a Password*. <http://www.nytimes.com/2012/01/18/us/teenagers-sharing-passwords-as-show-of-affection.html?pagewanted=all> [Accessed January 10, 2017].
- [80] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. M. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor.(2012) *How Does Your Password*

- Measure Up? The Effect of Strength Meters on Password Creation*. In Proceedings of the 21st USENIX Security Symposium, pages 65-80. USENIX Association, Aug. 2012.
- [81] A. Vance, D. Eargle, K. Ouimet, D. Straub.(2013) *Enhancing password security through interactive fear appeals: a web-based field experiment* Proceedings of the 46th Hawaii international conference on system sciences , pp. 2988-2997
- [82] Warut Khern-am-nuai, Yang, W. and Li, N., (2017). *Using Context-Based Password Strength Meter to Nudge Users' Password Generating Behavior: A Randomized Experiment*. In HICSS.
- [83] Egelman.S, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley. *Does My Password Go Up to Eleven?: The Impact of Password Meters on Password Selection*. (2013) In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 2379-2388. ACM, 2013
- [84] Gunson, N., Marshall, D., Morton, H. and Jack, M., (2011). *User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking*. Computers & Security, 30(4), pp.208-220.
- [85] Schougaard, D., Dragoni, N. and Spognardi, A., (2016). *Evaluation of Professional Cloud Password Management Tools*. In International Conference on Web Engineering (pp. 16-28). Springer International Publishing.
- [86] Chiasson, S., van Oorschot, P.C. and Biddle, R., (2006). *A Usability Study and Critique of Two Password Managers*. In USENIX Security Symposium (pp. 1-16).
- [87] Karole, A., Saxena, N. and Christin, N., (2010). *A Comparative Usability Evaluation of Traditional Password Managers*. In International Conference on Information Security and Cryptology (pp. 233-251). Springer, Berlin, Heidelberg.
- [88] Gray, J., Franqueira, V.N. and Yu, Y., (2016). *Forensically-sound analysis of security risks of using local password managers*. In Requirements Engineering Conference Workshops (REW), IEEE International (pp. 114-121). IEEE.
- [89] Zhao, R., Yue, C. and Sun, K., (2013). *Vulnerability and risk analysis of two commercial browser and cloud based password managers*. ASE Science Journal, 1(4), pp.1-15.
- [90] Li, Z., He, W., Akhawe, D. and Song, D., (2014). *The Emperor's New Password Manager: Security Analysis of Web-based Password Managers*. In USENIX Security Symposium (pp. 465-479).
- [91] Stobert, E. and Biddle, R., (2015). *Expert password management*. In International Conference on Passwords (pp. 3-20). Springer, Cham.

- [92] Nguyen, T.T.T. and Nguyen, Q.U., (2015). *An analysis of Persuasive Text Passwords*. In Information and Computer Science (NICS), 2015 2nd National Foundation for Science and Technology Development Conference on (pp. 28-33). IEEE.
- [93] Forget, A., Chiasson, S., van Oorschot, P.C. and Biddle, R., (2008). *Improving text passwords through persuasion*. In Proceedings of the 4th symposium on Usable privacy and security (pp. 1-12). ACM.
- [94] Mogire, N., Ogawa, M.B., Auernheimer, B. and Crosby, M.E., (2017). *Augmented Cognition for Continuous Authentication*. In International Conference on Augmented Cognition (pp. 342-356). Springer, Cham.
- [95] Segreti, S.M., Melicher, W., Komanduri, S., Melicher, D., Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L.F. and Mazurek, M.L., (2017). *Diversify to Survive: Making Passwords Stronger with Adaptive Policies*. In Symposium on Usable Privacy and Security (SOUPS).
- [96] Ranganayakulu, S., (2012). *A system-generated password and mnemonic approach to optimize the security and usability of text-based passwords*. (Doctoral dissertation, Clemson University).
- [97] Shay, R., Kelley, P.G., Komanduri, S., Mazurek, M.L., Ur, B., Vidas, T., Bauer, L., Christin, N. and Cranor, L.F., (2012). *Correct horse battery staple: Exploring the usability of system-assigned passphrases*. In Proceedings of the eighth symposium on usable privacy and security (p. 7). ACM.
- [98] Wright, N., Patrick, A.S. and Biddle, R., (2012). *Do you see your password?: applying recognition to textual passwords*. In Proceedings of the Eighth Symposium on Usable Privacy and Security (p. 8). ACM.
- [99] Barton, B.F. and Barton, M.S., (1984). *User-friendly password methods for computer-mediated information systems*. Computers & Security, 3(3), pp.186-195.
- [100] Yang, W., Li, N., Chowdhury, O., Xiong, A. and Proctor, R.W., (2016). *An empirical study of mnemonic sentence-based password generation strategies*. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 1216-1229). ACM.
- [101] Topkara, U., Atallah, M.J. and Topkara, M., (2007). *Passwords decay, words endure: Secure and re-usable multiple password mnemonics*. In Proceedings of the 2007 ACM symposium on Applied computing (pp. 292-299). ACM.
- [102] Kiesel, J., Stein, B. and Lucks, S., (2017). *A large-scale analysis of the mnemonic password advice*. In Proc. NDSS.

- [103] Camp, L.J., Abbott, J. and Chen, S., (2016). *CPasswords: Leveraging Episodic Memory and Human-Centered Design for Better Authentication*. In System Sciences (HICSS), 2016 49th Hawaii International Conference on (pp. 3656-3665). IEEE.
- [104] Renaud, K., McBryan, T. and Siebert, P., (2008). *Password cueing with cue (ink) blots*. IADIS Computer Graphics and Visualization, pp.74-81.
- [105] Al-Ameen, M.N., Wright, M. and Scielzo, S., (2015). *Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues*. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 2315-2324). ACM.
- [106] Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X., (2014). *The Tangled Web of Password Reuse*. In NDSS (Vol. 14, pp. 23-26).
- [107] Moshfeghian, S. and Ryu, Y.S., (2012). *A passport to password best practices*. Ergonomics in Design, 20(2), pp.23-29.
- [108] Shay, R., Bauer, L., Christin, N., Cranor, L.F., Forget, A., Komanduri, S., Mazurek, M.L., Melicher, W., Segreti, S.M. and Ur, B., (2015). *A spoonful of sugar?: The impact of guidance and feedback on password-creation behavior*. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 2903-2912). ACM.
- [109] Komanduri, S., Shay, R., Cranor, L.F., Herley, C. and Schechter, S.E., (2014). *Telepathwords: Preventing Weak Passwords by Reading Users' Minds*. In USENIX Security Symposium (pp. 591-606).
- [110] Karia, A.R. and Patankar, A.B., (2014). *Image Based Authentication Using Persuasive Cued Click Points*. International Journal of Engineering Research and Applications, 4(5), pp.179-185.
- [111] Furnell, S., Esmael, R., Yang, W. and Li, N., (2018). *Enhancing security behaviour by supporting the user*. Computers & Security, 75, pp.1-9.
- [112] Ciampa, M., (2013). *A comparison of password feedback mechanisms and their impact on password entropy*. Information Management & Computer Security, 21(5), pp.344-359.
- [113] Sasse, M.A., Brostoff, S. and Weirich, D., (2001). *Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security*. BT technology journal, 19(3), pp.122-131.
- [114] Habib, H., Colnago, J., Melicher, W., Ur, B., Segreti, S., Bauer, L., Christin, N. and Cranor, L., (2017). *Password creation in the presence of blacklists*. Proc. USEC.

- [115] Komanduri, S., Shay, R., Kelley, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F. and Egelman, S., (2011). *Of passwords and people: measuring the effect of password-composition policies*. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2595-2604). ACM.
- [116] Collis, J. and Hussey, R., (2013). *Business research: A practical guide for undergraduate and postgraduate students*. Macmillan International Higher Education.
- [117] Fogg, B.J., (2002). *Persuasive technology: using computers to change what we think and do*. Ubiquity, 2002(December), p.5.
- [118] Bishop, M., (1991). *Comparing authentication techniques*. In Proceedings of the Third Workshop on Computer Incident Handling (pp. 1-10).
- [119] Huh, J.H., Kim, H., Bobba, R.B., Bashir, M.N. and Beznosov, K., (2015). *On the memorability of system-generated PINs: Can chunking help?*. In SOUPS (pp. 197-209).
- [120] Carstens, D.S. and Malone, L.C., (2006). *Applying Chunking Theory in Organizational Password Guidelines*. Journal of Information, Information Technology & Organizations, 1.
- [121] Scott, C., Wynne, D. and Boonthum-Denecke, C., (2016). *Examining the Privacy of Login Credentials Using Web-Based Single Sign-on: Are We Giving Up Security and Privacy for Convenience?*. In Cybersecurity Symposium (CYBERSEC), 2016 (pp. 74-79). IEEE.
- [122] Sun, S.T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K. and Beznosov, K., (2011). *What makes users refuse web single sign-on?: an empirical investigation of OpenID*. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 4). ACM.
- [123] Krol, K., Philippou, E., De Cristofaro, E. and Sasse, M.A., (2015). *"They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking*. arXiv preprint arXiv:1501.04434.
- [124] Das, S., Russo, G., Dingman, A.C., Dev, J., Kenny, O. and Camp, L.J., (2017). *A qualitative Study on Usability and Acceptability of Yubico Security Key*. STAST, 2017
- [125] Al-Daraiseh, A.A., Al Omari, D., Al Hamid, H., Hamad, N. and Althemali, R., (2015). *Effectiveness of iPhones Touch ID: KSA case study*. Editorial Preface, 6(1).
- [126] Dasgupta, D., Roy, A. and Nag, A., (2017). *Biometric Authentication*. In Advances in User Authentication (pp. 38-40). Springer, Cham.
- [127] Sable, A.H., Talbar, S.N. and Dhirbasi, H.A., (2017). *Recognition of plastic surgery faces and the surgery types: An approach with entropy based scale invariant features*. Journal of King Saud University-Computer and Information Sciences.

- [128] Petsas, T., Tsirantonakis, G., Athanasopoulos, E. and Ioannidis, S., (2015). *Two-factor authentication: is the world ready?: quantifying 2FA adoption*. In Proceedings of the eighth european workshop on system security (p. 4). ACM.
- [129] Jermyn, I.H., Mayer, A., Monroe, F., Reiter, M.K. and Rubin, A.D., (1999). *The design and analysis of graphical passwords*. USENIX Association.
- [130] Dunphy, P. and Yan, J., (2007). *Do background images improve draw a secret graphical passwords?*. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 36-47). ACM.
- [131] Jebriel, S. and Poet, R., (2014). *Exploring the guessability of hand drawn images based on cultural characteristics*. In Computer Science and Information Technology (CSIT), 2014 6th International Conference on (pp. 5-13). IEEE.
- [132] A.J., Gibson, K.L., Mossop, E., Blaze, M. and Smith, J.M., (2010). *Smudge Attacks on Smartphone Touch Screens*. Woot, 10, pp.1-7.
- [133] Brostoff, S. and Sasse, M.A., (2000). *Are Passfaces more usable than passwords? A field trial investigation*. In People and Computers XIV—Usability or Else! (pp. 405-424). Springer, London.
- [134] Stobert, E. and Biddle, R., (2013). *Memory Retrieval and Graphical Passwords*. In Symposium on Usable Privacy and Security (SOUPS).
- [135] Chowdhury, S., Poet, R. and Mackenzie, L., (2013). *A comprehensive study of the usability of multiple graphical passwords*. In IFIP Conference on Human-Computer Interaction (pp. 424-441). Springer, Berlin, Heidelberg.
- [136] Biddle, R., Chiasson, S. and Van Oorschot, P.C., (2012). *Graphical passwords: Learning from the first twelve years*. ACM Computing Surveys (CSUR), 44(4), p.19.
- [137] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N., (2005). *PassPoints: Design and longitudinal evaluation of a graphical password system*. International journal of human-computer studies, 63(1-2), pp.102-127.
- [138] FIPS, (1985). *Password Usage*. Federal Information Processing Standards Publication. May 30.
- [139] Grassi, P.A., Perlner, R.A., Newton, E.M., Regenscheid, A.R., Burr, W.E., Richer, J.P., Lefkovitz, N.B., Danker, J.M. and Theofanos, M.F., (2017). *Digital Identity Guidelines: Authentication and Lifecycle Management* (No. Special Publication (NIST SP)-800-63B).

- [140] Renaud, K., Mayer, P., Volkamer, M. and Maguire, J., (2013). *Are graphical authentication mechanisms as strong as passwords?*. In 2013 Federated Conference on Computer Science and Information Systems (pp. 837-844). IEEE.
- [141] Renaud, K. and De Angeli, A., (2004). *My password is here! An investigation into visuo-spatial authentication mechanisms*. Interacting with computers, 16(6), pp.1017-1041.
- [142] Althubaiti, S. and Petrie, H., (2017). *Instructions for creating passwords: how do they help in password creation*. In Proceedings of the 31st British Computer Society Human Computer Interaction Conference (p. 55). BCS Learning & Development Ltd..
- [143] Corbin, J. and Strauss, A., (2008). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, 3rd Edition, 2008, p55
- [144] Seaman, C. (1999). *Qualitative methods in empirical studies of software engineering*. IEEE Transactions on Software Engineering, 25 (4), 557-572.
- [145] Glaser, B. (1978). *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*. Milley Valley, CA: Sociology Press. P. 73-79
- [146] Ha, E. and Wagner, D., (2013.) *Do Android users write about electric sheep? Examining consumer reviews in Google Play*. In Consumer Communications and Networking Conference (CCNC), 2013 IEEE, pp. 149-157, IEEE, 2013.
- [147] Yoganathan, D. and Kajanan, S., (2015). *Designing Fitness Apps Using Persuasive Technology A Text Mining Approach*. In Proceedings of the 18th Pacific Asia Conference on Information Systems, 2015.
- [148] Bowling, A., (2005). *Mode of questionnaire administration can have serious effects on data quality*. Journal of public health, 27(3), pp.281-291.
- [149] Hassenzahl, M., (2008). *User experience (UX): towards an experiential perspective on product quality*. In Proceedings of the 20th International Conference of the Association Francophone d'Interaction Homme-Machine IHM (Vol. 8, pp. 11-15).
- [150] Kirlappos, I., Parkin, S. and Sasse, M.A., (2014). *Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security*. In NDSS Workshop on Usable Security (USEC) .
- [151] Google, *Google Play Store*. Accessed: 25th Nov 2015.
- [152] Apple, *iTunes Apple Store*. Accessed: 25th Nov 2015.

- [153] Hofstede, G. and Bond, M.H., (1984). *Hofstede's culture dimensions: An independent validation using Rokeach's value survey*. Journal of cross-cultural psychology, 15(4), pp.417-433.
- [154] Henry, A., (2015). *Most Popular Password Manager: LastPass*, lifehacker, viewed 25th Nov 2015, <<https://lifehacker.com/5529133/five-best-password-managers/1679554433>>.
- [155] Roboform.com, *Password manager*. Accessed: 15 th April 2016.
- [156] Plautz, J., (2015). *The 12 Best Password Managers for Protecting Your Personal and Shared Accounts*. zapier, viewed 25th Nov 2015, <<https://zapier.com/blog/best-password-manager/>>
- [157] Ayalew, R., (2011). *The Paradox of Overfitting*. Master's thesis, Human Computer Interaction Programme, Uppsala University, 2011.
- [158] Pink, D.H., (2011). *Drive: The surprising truth about what motivates us*. New York: Penguin Group, Inc, vol. 138, p. 240.
- [159] Yang, H.C., (2013). *Bon Appetit for apps: young American consumers' acceptance of mobile applications*. Journal of Computer Information Systems, 53(3), pp.85-96.
- [160] Hassenzahl, M., Diefenbach, S. and GÄrritz, A., (2010). *Needs, affect, and interactive products-Facets of user experience*. Interacting with Computers, 22(5), pp.353-362.
- [161] Croyle, R.T., (2005). *Theory at a glance: a guide for health promotion practice*. Washington, DC: National Cancer Institute.
- [162] Egelman, S., Harbach, M. and Peer, E., (2016), May. *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 (pp. 5257-5261). ACM.
- [163] Ryan, R.M., Rigby, C.S. and Przybylski, A., (2006). *The motivational pull of video games: A self-determination theory approach*. Motivation and emotion, 30(4), pp.344-360.
- [164] Wohn, D.Y., (2013). *Gaming Habits and Self-determination: Conscious and Non-conscious Paths to Behavior Continuance*. Michigan State University. Media and Information Studies.
- [165] Ngoqo, B. and Flowerday, S.V., (2015). *Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users*. Computers & security, 53, pp.132-142.
- [166] Rhee, H.S., Kim, C. and Ryu, Y.U., (2009). *Self-efficacy in information security: Its influence on end users' information security practice behavior*. Computers & Security, 28(8), pp.816-826.

- [167] Gundu, T. and Flowerday, S.V., (2012), August. *The enemy within: A behavioural intention model and an information security awareness process*. In Information Security for South Africa (ISSA), 2012 (pp. 1-8). IEEE.
- [168] Gagn  , M., (2009). *A model of knowledge-sharing motivation*. Human Resource Management: Published in Cooperation with the School of Business Administration, The University of Michigan and in alliance with the Society of Human Resources Management, 48(4), pp.571-589.
- [169] Bhattacharjee, A. and Park, S.C., (2014). *Why end-users move to the cloud: a migration-theoretic analysis*. European Journal of Information Systems, 23(3), pp.357-372.
- [170] Zhang, K.Z., Cheung, C.M. and Lee, M.K., (2012). *Online service switching behavior: the case of blog service providers*. Journal of Electronic Commerce Research, 13(3), p.18
- [171] Zengyan, C., Yinping, Y. and Lim, J., (2009), January. *Cyber migration: An empirical investigation on factors that affect users' switch intentions in social networking sites*. In 2009 42nd Hawaii International Conference on System Sciences (pp. 1-11). IEEE.
- [172] Schreiner, M. and Hess, T., (2015). *Examining the role of privacy in virtual migration: The case of whatsapp and threema*. In Proceedings of the 21st Americas Conference on Information Systems, AMCIS '15, 2015.
- [173] Wiklund-Engblom, A., Hassenzahl, M., Bengs, A. and Sperring, S., (2009), August. *What needs tell us about user experience?* In IFIP Conference on Human-Computer Interaction (pp. 666-669). Springer, Berlin, Heidelberg.
- [174] Egelman, S., Jain, S., Portnoff, R.S., Liao, K., Consolvo, S. and Wagner, D., (2014), November. *Are you ready to lock?*. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 750-761). ACM.
- [175] Szalma, J.L., (2014). *On the application of motivation theory to human factors/ergonomics: Motivational design principles for human-technology interaction*. Human factors, 56(8), pp.1453-1471.
- [176] Zhang-Kennedy, L., Fares, E., Chiasson, S. and Biddle, R., (2016), June. *Geo-Phisher: the design and evaluation of information visualizations about internet phishing trends*. In 2016 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-12). IEEE.
- [177] Machuletz, D., Sendt, H., Laube, S. and B  hme, R., (2016). *Users protect their privacy if they can: Determinants of webcam covering behavior*. In Proceedings of the European Workshop on Usable Security (EuroUSEC'16). Internet Society, Reston, VA, USA.

- [178] O’keefe, R.M. and McEachern, T., (1998). *Web-based customer decision support systems*. Communications of the ACM, 41(3), pp.71-78.
- [179] Detlor, B. and Arsenault, C., (2002). *Web information seeking and retrieval in digital library contexts: towards an intelligent agent solution*. Online Information Review, 26(6), pp.404-412.
- [180] HÃd’ubl, G. and Trifts, V., (2000). *Consumer decision making in online shopping environments: The effects of interactive decision aids*. Marketing science, 19(1), pp.4-21.
- [181] . Komiak, S. and Benbasat, I., (2004). *Comparing persuasiveness of different recommendation agents as customer decision support systems in electronic commerce*. In Proc. of the 2004 IFIP International Conference on Decision Support Systems.
- [182] . Mandl, M., Felfernig, A., Teppan, E. and Schubert, M., (2011). *Consumer decision making in knowledge-based recommendation*. Journal of Intelligent Information Systems, 37(1), pp.1-22.
- [183] . Pu, P. and Chen, L., (2008). *User-involved preference elicitation for product search and recommender systems*. AI magazine, 29(4), p.93.
- [184] . Blom, J., (2002), April. *A theory of personalized recommendations*. In CHI’02 Extended Abstracts on Human Factors in Computing Systems (pp. 540-541). ACM.
- [185] . Felfernig, A., Jeran, M., Ninaus, G., Reinfrank, F., Reiterer, S. and Stettinger, M., (2014). *Basic approaches in recommendation systems*. In Recommendation Systems in Software Engineering (pp. 15-37). Springer, Berlin, Heidelberg.
- [186] . McCarthy, K., McGinty, L., Smyth, B. and Reilly, J., (2005), August. *A live-user evaluation of incremental dynamic critiquing*. In International Conference on Case-Based Reasoning (pp. 339-352). Springer, Berlin, Heidelberg.
- [187] . McCarthy, K., Reilly, J., McGinty, L. and Smyth, B., (2004), August. *Thinking positively explanatory feedback for conversational recommender systems*. In Proceedings of the European Conference on Case-Based Reasoning (ECCBR-04) Explanation Workshop (pp. 115-124).
- [188] . Torrens, M., Faltings, B. and Pu, P., (2002). *Smartclients: Constraint satisfaction as a paradigm for scaleable intelligent information systems*. Constraints, 7(1), pp.49-69.
- [189] . Silva, M.N., Marques, M.M. and Teixeira, P.J., (2014). *Testing theory in practice: The example of self-determination theory-based interventions*. European Health Psychologist, 16(5), pp.171-180.

- [190] . Staunton, L., Gellert, P., Knittle, K. and Sniehotta, F.F., (2014). *Perceived control and intrinsic vs. extrinsic motivation for oral self-care: A full factorial experimental test of theory-based persuasive messages*. Annals of Behavioral Medicine, 49(2), pp.258-268.
- [191] . Zhang-Kennedy, L., Chiasson, S. and Biddle, R., (2014), May. *Stop clicking on "update later": Persuading users they need up-to-date antivirus protection*. In International Conference on Persuasive Technology (pp. 302-322). Springer, Cham.
- [192] . Sheila, M., Faizal, M.A. and Shahrin, S., (2015). *Dimension of mobile security model: mobile user security threats and awareness*. International Journal, 9(1), pp.66-85.
- [193] . Beautement, A., Sasse, M.A. and Wonham, M., (2009), August. *The compliance budget: managing security behaviour in organisations*. In Proceedings of the 2008 New Security Paradigms Workshop (pp. 47-58). ACM.
- [194] . Ryan, R.M. and Deci, E.L., (2000). *Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being*. American psychologist, 55(1), p.68.
- [195] . Humaidi, N. and Balakrishnan, V., (2013). *Exploratory factor analysis of user's compliance behaviour towards health information system's security*. Journal of Health & Medical Informatics, 4(2), pp.2-9.
- [196] . Deterding, S., Dixon, D., Khaled, R. and Nacke, L., (2011), September. *From game design elements to gamefulness: defining gamification*. In Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments (pp. 9-15). ACM.
- [197] . Jones, C.M., McCarthy, R.V., Halawi, L. and Mujtaba, B., (2010). *Utilizing the technology acceptance model to assess the employee adoption of information systems security measures*. Issues in Information Systems, 11(1), p.9.
- [198] . Siponen, M., Pahlila, S. and Mahmood, M.A., (2010). *Compliance with information security policies: An empirical investigation*. Computer, 43(2).
- [199] . Swarna Nantha, Y., (2013). *Intrinsic motivation: how can it play a pivotal role in changing clinician behaviour?*. Journal of health organization and management, 27(2), pp.266-272.
- [200] . Lin, H.F., (2007). *Effects of extrinsic and intrinsic motivation on employee knowledge sharing intentions*. Journal of information science, 33(2), pp.135-149.
- [201] Schell, J., (2014). *The Art of Game Design: A Book of Lenses*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.. isbn: 0-12-369496-5.

- [202] Deci, E.L. and Ryan, R.M., (2002). *Overview of self-determination theory: An organismic dialectical perspective*. Handbook of self-determination research, pp.3-33.
- [203] Ross, B., Jackson, C., Miyake, N., Boneh, D. and Mitchell, J.C., (2005), August. *Stronger Password Authentication Using Browser Extensions*. In USENIX Security Symposium (pp. 17-32).
- [204] Kreijns, K., Vermeulen, M., Van Acker, F. and Van Buuren, H., (2014). *Predicting teachers' use of digital learning materials: combining self-determination theory and the integrative model of behaviour prediction*. European Journal of Teacher Education, 37(4), pp.465-478.
- [205] Williams, G.C., Patrick, H., Niemiec, C.P., Ryan, R.M., Deci, E.L. and Lavigne, H.M., (2011). *The smoker's health project: a self-determination theory intervention to facilitate maintenance of tobacco abstinence*. Contemporary clinical trials, 32(4), pp.535-543.
- [206] Gumussoy, C.A., Kaya, A. and Ozlu, E., (2018). *Determinants of Mobile Banking Use: An Extended TAM , Mobility Access, Compatibility, Perceived Self-efficacy and Subjective Norms*. In Industrial Engineering in the Industry 4.0 Era (pp. 225-238). Springer, Cham.
- [207] Yang, S., Chen, Y. and Wei, J., (2015). *Understanding consumers' web-mobile shopping extension behavior: A trust transfer perspective*. Journal of computer information systems, 55(2), pp.78-87.
- [208] Gundu, T. and Flowerday, S.V., (2013). *Ignorance to awareness: Towards an information security awareness process*. SAIEE Africa Research Journal, 104(2), pp.69-79.
- [209] Mou, J., Cohen, J. and Kim, J., (2017). *A Meta-Analytic Structural Equation Modeling Test of Protection Motivation Theory in Information Security Literature*. ICIS 2017: Transforming Society with Digital Innovation.
- [210] Park, S.C. and Ryoo, S.Y., (2013). *An empirical investigation of end-users' switching toward cloud computing: A two-factor theory perspective*. Computers in Human Behavior, 29(1), pp.160-170.
- [211] Yee, K.P. and Sitaker, K., (2006), July. *Passpet: convenient password management and phishing protection*. In Proceedings of the second symposium on Usable privacy and security (pp. 32-43). ACM.
- [212] Miltgen, C.L., Popovic, A. and Oliveira, T., (2013). *Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context*. Decision Support Systems, 56, pp.103-114.

- [213] Mou, Y. and Lin, C.A., (2015). *Exploring podcast adoption intention via perceived social norms, interpersonal communication, and theory of planned behavior*. Journal of Broadcasting & Electronic Media, 59(3), pp.475-493.
- [214] Thompson, N., McGill, T.J. and Wang, X., (2017). *"Security begins at home": Determinants of home computer and mobile device security behavior*. computers & security, 70, pp.376-391.
- [215] Sun, Y., Liu, D., Chen, S., Wu, X., Shen, X.L. and Zhang, X., (2017). *Understanding users' switching behavior of mobile instant messaging applications: An empirical study from the perspective of push-pull-mooring framework*. Computers in Human Behavior, 75, pp.727-738.
- [216] Chang, I.C., Liu, C.C. and Chen, K., (2014). *The push, pull and mooring effects in virtual migration for social networking sites*. Information Systems Journal, 24(4), pp.323-346.
- [217] Vafaei-Zadeh, A., Ramayah, T., Wong, W.P. and Md Hanifah, H., (2018). *Modelling Internet security software usage among undergraduate students: A necessity in an increasingly networked world*. VINE Journal of Information and Knowledge Management Systems, 48(1), pp.2-20.
- [218] Gurung, A., Luo, X. and Liao, Q., (2009). *Consumer motivations in taking action against spyware: an empirical investigation*. Information Management & Computer Security, 17(3), pp.276-289.
- [219] Chen, X., Wu, D., Chen, L. and Teng, J.K., (2018). *Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables*. Information & Management, 55(8), pp.1049-1060.
- [220] Djeni, I. and Erbilek, M., (2017), September. *Intention to use biometric systems among international students in Cyprus*. In Computational Intelligence and Communication Networks (CICN), 2017 9th International Conference on (pp. 229-235). IEEE.
- [221] Fishbein, M. and Ajzen, I., 2011. *Predicting and Changing Behavior: The Reasoned Action Approach*. Psychology Press.
- [222] Hovav, A. and Putri, F.F., 2016. *This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy*. Pervasive and Mobile Computing, 32, pp.35-49.
- [223] Fan, L. and Suh, Y.H., 2014. *Why do users switch to a disruptive technology? An empirical study based on expectation-disconfirmation theory*. Information & Management, 51(2), pp.240-248.

- [224] Suh, J.-H. and S.-G. Chang (2013). *An Empirical Study on the Enterprise Cloud Service Adoption*. In: Proceedings of the Pacific Asia Conference on Information Systems (PACIS). Jeju Island, Korea
- [225] Cialdini, R.B., Reno, R.R. and Kallgren, C.A., (1990). *A focus theory of normative conduct: recycling the concept of norms to reduce littering in public places*. Journal of personality and social psychology, 58(6), p.1015.
- [226] Tu, Z., Yuan, Y. and Archer, N., (2014.) *Understanding user behaviour in coping with security threats of mobile device loss and theft*. International Journal of Mobile Communications, 12(6), pp.603-623.
- [227] Lee, Y. and Larsen, K.R., (2009.) *Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software*. European Journal of Information Systems, 18(2), pp.177-187.
- [228] Vasileiadis, A., (2014.) *Security concerns and trust in the adoption of m-commerce*. Social Technologies, 4(1), pp.179-191.
- [229] Pham, H-C., Brennan, L., and Richardson. J. (2017). *Review of behavioural theories in security compliance and research challenges*. Proceedings of the Informing Science and Information Technology Education Conference, Vietnam, pp. 65-76. Santa Rosa, CA: Informing Science Institute.
- [230] Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J., (2014). *Variables influencing information security policy compliance: a systematic review of quantitative studies*. Information Management & Computer Security, 22(1), pp.42-75.
- [231] Vincent, J. (2017). *99.6 percent of new smartphones run Android or iOS - While BlackBerry's market share is a rounding error*. [Online] The verge, viewed 4 Oct. 2018, <<https://www.theverge.com/2017/2/16/14634656/android-ios-market-share-blackberry-2016>>
- [232] Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P., (2015). *What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors*. MIS Quarterly, 39(4), pp.837-864.
- [233] Zhou, T., (2012). *Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk*. Journal of Electronic Commerce Research, 13(2), p.135.
- [234] Kim, D.J., Steinfield, C. and Lai, Y.J., (2008). *Revisiting the role of web assurance seals in business-to-consumer electronic commerce*. Decision Support Systems, 44(4), pp.1000-1015.

- [235] Ernst, C.P.H., (2015). *Risk hurts fun: The influence of perceived privacy risk on social network site usage*. In Factors Driving Social Network Site Usage (pp. 45-56). Springer Gabler, Wiesbaden.
- [236] Kim, B., (2010). *An empirical investigation of mobile data service continuance: Incorporating the theory of planned behavior into the expectation-confirmation model*. Expert systems with applications, 37(10), pp.7033-7039.
- [237] Mwagwabi, F., (2015). *A protection motivation theory approach to improving compliance with password guidelines*. Doctoral dissertation, Murdoch University..
- [238] Woon, I., Tan, G.W. and Low, R., (2005). *A protection motivation theory approach to home wireless security*. ICIS 2005 proceedings, p.31.
- [239] Lee, J.M. and Rha, J.Y., (2016). *Personalization-privacy paradox and consumer conflict with the use of location-based mobile commerce*. Computers in Human Behavior, 63, pp.453-462.
- [240] Ramayah, T., Rouibah, K., Gopi, M. and Rangel, G.J., (2009.) *A decomposed theory of reasoned action to explain intention to use Internet stock trading among Malaysian investors*. Computers in Human Behavior, 25(6), pp.1222-1230.
- [241] Little, R.J., 1988. *A test of missing completely at random for multivariate data with missing values*. Journal of the American statistical Association, 83(404), pp.1198-1202.
- [242] George, D., (2011). *SPSS for windows step by step: A simple study guide and reference*, 17.0 update, 10/e. Pearson Education India.
- [243] Tabachnick, B.G. and Fidell, L.S., (2013). *Using multivariate statistics*, sixth edition. Boston: Pearson
- [244] Hair, J., Black, W., Babin, B., and Anderson, R. (2010). *Multivariate data analysis* (7th ed.): Prentice-Hall, Inc. Upper Saddle River, NJ, USA.
- [245] Kline, R.B., (2015). *Principles and practice of structural equation modelling*. New York: Guilford publications.
- [246] Zhu, W., (2000). *Which should it be called: Convergent validity or discriminant validity?*. Research quarterly for exercise and sport, 71(2), pp.190-194.
- [247] Fornell, C. and Larcker, D.F., (1981). *Evaluating structural equation models with unobservable variables and measurement error*. Journal of marketing research, pp.39-50.
- [248] Gaskin, J. (2012). *Validity Master*. Gaskination's StatWiki, viewed 21 Nov 2017, <<https://statwiki.kolobkreations.com> >

- [249] Hooper, D., Coughlan, J. and Mullen, M.R., (2008). *Structural Equation Modelling: Guidelines for Determining Model Fit*. Electronic Journal of Business Research Methods, 6(1), pp.53-60.
- [250] Byrne, B.M. (2013) *Structural equation modelling with AMOS: basic concepts, applications, and programming*, . 2nd edn. New York: Taylor & Francis Group.
- [251] Alalwan, A.A., Dwivedi, Y.K., Rana, N.P. and Simintiras, A.C., (2016). *Jordanian consumers' adoption of telebanking: Influence of perceived usefulness, trust and self-efficacy*. International Journal of Bank Marketing, 34(5), pp.690-709.
- [252] Hsieh, Y.C., Hsieh, J.K. and Feng, Y.C., (2011). *Switching between social media: The role of motivation and cost*. In 2011 2nd International Conference on Economics, Business and Management (Vol. 22, pp. 92-96).
- [253] Featherman, M.S. and Pavlou, P.A., (2003). *Predicting e-services adoption: a perceived risk facets perspective*. International journal of human-computer studies, 59(4), pp.451-474.
- [254] Kim, D.J., Ferrin, D.L. and Rao, H.R., (2008). *A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents*. Decision support systems, 44(2), pp.544-564.
- [255] Hsieh, P.J., (2015). *Physicians' acceptance of electronic medical records exchange: An extension of the decomposed TPB model with institutional trust and perceived risk*. International journal of medical informatics, 84(1), pp.1-14.
- [256] Ryu, H.S., (2018). January. *Understanding Benefit and Risk Framework of Fintech Adoption: Comparison of Early Adopters and Late Adopters*. In Proceedings of the 51st Hawaii International Conference on System Sciences.
- [257] supergenpass. (2016). *SuperGenPass*. [ONLINE] Available at: <http://supergenpass.com/genpass/>. [Accessed 8 August 2018].
- [258] Aurigemma, S., Mattson, T. and Leonard, L., (2017), January. *So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications?*. In Proceedings of the 50th Hawaii International Conference on System Sciences.
- [259] Butler, J.M., (2012). *Privileged password sharing: "root" of all evil*. SANS Analyst Program, pp.1-12.
- [260] Kissell, J. (2016). *Take control of your passwords*. Take Control Books.

- [261] Walkup, E. (2016). *The Password Problem* (No. SAND2016–5208T). Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States).
- [262] Fagan, M. and Khan, M.M.H., (2016). *Why do they do what they do?: A study of what motivates users to (not) follow computer security advice*. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) (pp. 59-75).
- [263] Gugathas, T., (2016). *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.
- [264] Zanker, M., Fuchs, M., Hopken, W., Tuta, M. and Muller, N., (2008.) *Evaluating recommender systems in tourism-a case study from Austria*. Information and communication technologies in tourism 2008, pp.24-34.
- [265] AdMob.(2010)*AdMob Mobile Metrics Report*. AdMob, viewed 21 Nov 2017, <https://www.wired.com/images_blogs/gadgetlab/2010/02/admob-mobile-metrics-jan-10.pdf>
- [266] Stone, D.N., Deci, E.L. and Ryan, R.M., (2009). *Beyond talk: Creating autonomous motivation through self-determination theory*. Journal of General Management, 34(3), pp.75-91.
- [267] Su, Y.L. and Reeve, J., (2011). *A meta-analysis of the effectiveness of intervention programs designed to support autonomy*. Educational Psychology Review, 23(1), pp.159-188.
- [268] Reeve, J., (2016). *Autonomy-supportive teaching: What it is, how to do it*. In Building autonomous learners (pp. 129-152). Springer, Singapore.
- [269] Straton, R.G. and Catts, R.M., (1980). *A comparison of two, three and four-choice item tests given a fixed total number of choices*. Educational and Psychological Measurement, 40(2), pp.357-365.
- [270] Maxwell, S., (2005). *Hyperchoice and high prices: an unfair combination*. Journal of Product & Brand Management, 14(7), pp.448-454.
- [271] Andersen, S.M., Chen, S. and Carter, C., (2000). *Fundamental human needs: Making social cognition relevant*. Psychological inquiry, 11(4), pp.269-275.
- [272] Hasan, A., (2014). *Managing students' motivation: An empirical study from self-determination perspective*. In 2nd International Conference on Management from an Islamic Perspective (ICMIP-2 2014), International Islamic University Malaysia.
- [273] Young, H.P., (2009). *Innovation diffusion in heterogeneous populations: Contagion, social influence, and social learning*. American economic review, 99(5), pp.1899-1924.

- [274] Bakx, A., Van Houtert, T., Brand, M.V.D. and Hornstra, L., (2017). *A comparison of high-ability pupils' views vs. regular ability pupils' views of characteristics of good primary school teachers*. Educational Studies, 45(1), pp. 1-22.
- [275] Harackiewicz, J.M., Manderlink, G. and Sansone, C., (1984). *Rewarding pinball wizardry: Effects of evaluation and cue value on intrinsic interest*. Journal of Personality and Social Psychology, 47(2), p.287.
- [276] Jussim, L., Soffin, S., Brown, R., Ley, J. and Kohlhepp, K.,(1992). *Understanding reactions to feedback by integrating ideas from symbolic interactionism and cognitive evaluation theory*. Journal of personality and social psychology, 62(3), p.402.
- [277] E. M. Thuen,(2007). *Learning environment, students' coping styles and emotional and behavioural problems*. PhD thesis, Department of Psycosocial Science, Faculty of Psychology, The University of Bergen. .
- [278] International Data Corporation (IDC Corporate USA),(2018). *Smartphone OS Market Share, 2017 Q1*,International Data Corporation, viewed 10 January 2018 <<https://www.idc.com/promo/smartphone-market-share/os>. >
- [279] Kim,E.(2016). *The meteoric rise of iOS and Android in one chart*.Businessinsider,viewed 10 January 2018 < <http://uk.businessinsider.com/iosand-android-dominate-marketshare-2016-2?r=US&IR=T>.>
- [280] Rosenthal, R. and Rosnow, R.L., (2009). *Artifacts in behavioral research: Robert Rosenthal and Ralph L. Rosnow's classic books*. Oxford University Press.
- [281] Shiv, B., Carmon, Z. and Ariely, D., (2005). *Placebo effects of marketing actions: Consumers may get what they pay for*. Journal of marketing Research, 42(4), pp.383-393.
- [282] Miller, F.G., Colloca, L. and Kaptchuk, T.J., (2009). *The placebo effect: illness and interpersonal healing*. Perspectives in biology and medicine, 52(4), p.518.
- [283] Shropshire, J., Warkentin, M. and Sharma, S., (2015). *Personality, attitudes, and intentions: Predicting initial adoption of information security behavior*. Computers & Security, 49, pp.177-191.
- [284] Bonini, D., (2005). *A model of trust in the work of an air traffic controller*. Doctoral dissertation, Trinity College Dublin.
- [285] March, J.G., (1995.) *The future, disposable organizations and the rigidities of imagination*. Organization, 2(3-4), pp.427-440.

- [286] Shim, S. and Lee, Y., (2011). *Consumer's perceived risk reduction by 3D virtual model*. International Journal of Retail & Distribution Management, 39(12), pp.945-959.
- [287] Siponen, M. and Baskerville, R., (2018). *Intervention Effect Rates as a Path to Research Relevance: Information Systems Security Example*. Journal of the Association for Information Systems, 19(4), pp.247-265.