

Users' Perceptions Regarding Password Policies

D.T Fredericks

April 2018

Users' Perceptions Regarding Password Policies

By

Damian Todd Fredericks

Dissertation

Submitted in fulfilment of the requirements for the degree

Masters in Information Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela University

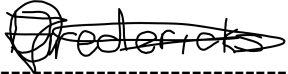
Supervisor: Prof Lynn Futcher

Co-supervisor: Prof Kerry-Lynn Thomson

April 2018

Declaration

I, Damian Todd Fredericks (s212212435), hereby declare that the dissertation, entitled Users' Perceptions Regarding Password Policies, which I have submitted at the Nelson Mandela University, is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University or for another qualification.

A handwritten signature in black ink, appearing to read "D. Fredericks", written over a horizontal dashed line.

Damian Todd Fredericks

Abstract

Information is considered a valuable asset to most organisations and is often exposed to various threats which exploit its confidentiality, integrity and availability (CIA). Identification and Authentication are commonly used to help ensure the CIA of information. This research study specifically focused on password-based authentication. Passwords are used to log into personal computers, company computers, email accounts, bank accounts and various software systems and mobile applications. Passwords act like a protective barrier between a user and their personal and company information, and remain the most cost-effective and most efficient method to control access to computer systems.

An extensive content analysis was conducted regarding the security of passwords, as well as users' password management coping strategies. It was determined that very little research has been conducted in relation to users' perceptions towards password policies. The problem identified by this research is that organisations often implement password policy guidelines without taking into consideration users' perceptions regarding such guidelines. This could result in users adopting various password management coping strategies. This research therefore aimed to determine users' perceptions with regard to current password-related standards and best practices (password policy guidelines). Standards and best practices such as ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), NIST SP 800-63B (2016) and the SANS Password Protection Policy (2014b) were studied in order to determine the common elements of password policies. This research argued that before organisations implement password policy guidelines, they need to determine users' perceptions towards such guidelines. It was identified that certain human factors such as human memory, attitude and apathy often cause users to adopt insecure coping strategies such as Reusing Passwords, Writing Down Passwords and Not Changing Passwords.

This research included a survey which took the form of a questionnaire. The aim of the survey was to determine users' perceptions towards common elements of password policies and to determine the coping strategies users commonly adopt. The survey included questions related to the new NIST SP 800-63B (2016) that sought to determine users' perceptions towards these new NIST password policy

guidelines. Findings from the survey indicated that respondents found the new NIST guidelines to be helpful, secure and easier to adhere to. Finally, recommendations regarding password policies were presented based on the common elements of password policies and users' perceptions of the new NIST password guidelines. These recommendations could help policy makers in the implementation of new password policies or the revision of current password policies.

Acknowledgements

I wish to express my sincere gratitude to the following:

Lord Jesus Christ for giving the strength and knowledge throughout the course of completing this dissertation.

Prof. Lynn Fatcher, my supervisor: for her valuable guidance, meticulous attention to detail and believing in me throughout this study. I have felt very honoured to have you as my supervisor.

Prof. Kerry-Lynn Thomson, my co-supervisor: for her valuable guidance and meticulous attention to detail throughout this study. I profoundly appreciated your input.

The financial assistance of the National Research Funding (NRF) is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors, and are not necessarily to be attributed to the NRF.

My loving family: My mother and father, brother and sister for constant support and encouragement throughout this study.

Table of Contents

Chapter 1 : Introduction	1
1.1 Background.....	1
1.2 Problem Area.....	2
1.3 Research Objectives	5
1.4 Research Methods	6
1.4.1 Literature Review	6
1.4.2 Survey.....	6
1.4.3 Content Analysis.....	7
1.4.4 Argumentation	7
1.5 Delineation and Limitations	8
1.6 Chapter Outline	8
1.7 Related Publications.....	10
1.8 Conclusion	10
Chapter 2 : Understanding Passwords.....	11
2.1 Introduction	11
2.2 Existing Password Research	12
2.2.1 Password Security and Strength	14
2.2.2 Password Threats	17
2.2.3 Password Management Lifecycle.....	18
2.2.3.1 Password Generation	18
2.2.3.2 Password Maintenance	21
2.2.3.3 Password Authentication	21
2.2.4 Password Policies	22
2.2.5 Password Coping Strategies	23
2.2.6 Human Factors	24
2.2.7 Alternative Methods	24
2.3 Conclusion	26
Chapter 3 : Password Policies	28
3.1 Introduction	28
3.2 Password Policy Standards and Best Practices	29
3.2.1 ISO/IEC 27002.....	29
3.2.2 NIST SP 800-118	32
3.2.3 NIST SP 800-63-2	34
3.2.4 NIST SP 800-63B	36

3.2.5	SANS Password Protection Policy.....	39
3.3	Summary of Common Elements.....	41
3.4	Password Policy Guideline Implementation	44
3.5	Conclusion	46
Chapter 4 :	Human Factors Relating to Passwords	48
4.1	Introduction	48
4.2	Key Human Factors.....	49
4.2.1	Human Memory	49
4.2.1.1	Password Length and Complexity	51
4.2.1.2	Password Expiration	51
4.2.1.3	Password History.....	52
4.2.1.4	Password Protection	52
4.2.2	Attitude and Apathy	53
4.2.2.1	Password Length and Complexity	54
4.2.2.2	Password Expiration	54
4.2.2.3	Password History.....	54
4.2.2.4	Password Protection	55
4.3	Password Coping Strategies	55
4.3.1	Reusing Passwords	57
4.3.2	Writing Down Passwords	60
4.3.3	Creating Weak Passwords.....	62
4.3.4	Not Changing Passwords.....	63
4.3.5	Password Managers and Single Sign-On	64
4.4	Education, Training and Awareness	65
4.5	Conclusion	68
Chapter 5 :	Research Design	69
5.1	Introduction	69
5.2	Research Approach	69
5.2.1	Deductive Reasoning.....	69
5.2.2	Inductive Reasoning	70
5.3	Research Process.....	70
5.3.1	Literature Review	72
5.3.2	Content Analysis.....	73
5.3.3	Argumentation	73
5.3.4	Survey.....	74
5.4	Sampling Techniques.....	74

5.5	Data Collection and Analysis	76
5.6	Respondents and Ethical Consent.....	77
5.7	Questionnaire Design.....	78
5.7.1	Survey Objective 1.....	80
5.7.2	Survey Objective 2.....	81
5.7.3	Survey Objective 3.....	81
5.8	Conclusion.....	82
Chapter 6 : Results and Findings		83
6.1	Introduction	83
6.2	Research Study Demographics.....	83
6.3	Sample Password Policy Results and Findings	84
6.4	Behaviour and Coping Strategies Results and Findings	89
6.5	Comparison of Employee and Student/Scholar Group.....	95
6.6	Conclusion.....	108
Chapter 7 : Interpretation and Discussion		110
7.1	Introduction	110
7.2	NIST SP 800 63B (2016) and NIST SP 800 63B (2017).....	110
7.3	Perceptions of Common Password Policy Elements.....	112
7.4	NIST SP800-63B Results and Findings	113
7.5	Discussion of NIST SP 800-63B (2016).....	115
7.5.1	Password Length	116
7.5.2	Password Complexity	117
7.5.3	Password Expiration	117
7.5.4	Password Protection	118
7.6	Password Policy Recommendations.....	120
7.6.1	Password Length	120
7.6.2	Password Complexity	121
7.6.3	Password Expiration	121
7.6.4	Password History.....	122
7.6.5	Password Protection	122
7.6.6	Password Coping Strategies	122
7.7	Conclusion.....	123
Chapter 8 : Conclusion.....		124
8.1	Introduction	124
8.2	Summary of Chapters.....	125
8.3	Meeting the Research Objectives	127

8.4	Contribution of Research	129
8.5	Research Limitations	129
8.6	Suggestions for Future Research.....	129
8.7	Epilogue.....	130
References		131
Appendix A1: Questionnaire		142
Appendix A2: Sample Password Policy		147
Appendix B: Raw Data		149
Appendix C: HAISA Paper.....		155
Appendix D: Proof Reader Declaration		163

List of Tables

Table 1.1: Research Objectives	5
Table 1.2: Survey Objectives	7
Table 2.1: Common Password Themes	14
Table 3.1: ISO/IEC 27002 Common Elements	32
Table 3.2: NIST SP 800-118 Common Elements	34
Table 3.3: NIST SP 800- 63-2 Password and Verifier Requirements	35
Table 3.4: NIST SP 800-63-2 Common Elements	36
Table 3.5: NIST SP 800-63B Common Elements	38
Table 3.6: SANS Common Elements	40
Table 3.7: Common Elements of Password Policies	41
Table 3.8: Comparison Between Various NIST Standards	43
Table 3.9: Microsoft, Apple and Google Password Policies	45
Table 5.1: Survey Objectives Linked to Secondary Objectives	80
Table 5.2: Survey Objective 1 Questions	80
Table 5.3: Survey Objective 2 Questions	81
Table 5.4: Survey Objective 3 Questions	82
Table 6.1: Research Study Demographic Results (n=75)	83
Table 6.2: Password Minimum Length of 8 (n=75)	84
Table 6.3: Password Maximum Length of 16 (n=75)	84
Table 6.4: Increased Password Maximum Length of 64 (n=75)	85
Table 6.5: Password Composition Requirements (n=74)	86
Table 6.6: Emojis and Spaces in Passwords (n=74)	86
Table 6.7: Password Change (n=74)	87
Table 6.8: General Password Recommendations (n=75)	87
Table 6.9: Password checking (n=75)	87
Table 6.10: Password Policy (n=75)	88
Table 6.11: Password Reuse (n=75)	89
Table 6.12: Password Reuse Reason (n=70)	90
Table 6.13: Password Generation Strategies (n=75)	90
Table 6.14: Password Composition Requirements (n=75)	91
Table 6.15: Password Tracking (n=75)	92
Table 6.16: Password Coping Strategies (n=75)	92
Table 6.17: Single Sign-On (n=75)	93
Table 6.18: Awareness or Education on Passwords (n=75)	93
Table 6.19: Awareness and Education Programmes Attended (n=20)	94
Table 7.1: NIST SP 800-63B(2016) and NIST SP 800-63B(2017)	111
Table 7.2: Perceptions Towards Sample Password Policy	112
Table 7.3: Minimum Password Length	114
Table 7.4: Maximum Password Length	114
Table 7.5: Password Composition Requirements	114
Table 7.6: ASCII Characters	114
Table 7.7: Password Expiration	115
Table 7.8: System Checking of Passwords	115
Table 7.9: Perceptions Regarding NIST SP 800-63B (2016)	116
Table 7.10: Password Policy Recommendations	120

List of Figures

Figure 2.1: McCumber Model (McCumber p.136,2004).....	16
Figure 2.2: Password Management Lifecycle (adapted from (Choong, 2014))	18
Figure 2.3: Apple Password Requirements (Apple, 2017)	19
Figure 2.4: Microsoft Password Requirements (Microsoft, 2017b).....	20
Figure 2.5: Google Password Requirements (Google, 2017b)	20
Figure 5.1: Research Process	71
Figure 5.2: Types of Questionnaires (Saunders et al p.420., 2012)	76
Figure 6.1: Question 2.1 Results	95
Figure 6.2: Question 2.2 Results	96
Figure 6.3: Question 2.3 Results	97
Figure 6.4: Question 2.5 Results	98
Figure 6.5: Question 2.6 Results	98
Figure 6.6: Question 2.7 Results	99
Figure 6.7: Question 2.9 Results	100
Figure 6.8: Question 3.1a Results	101
Figure 6.9: Question 3.2 Results	101
Figure 6.10: Question 3.3 Results	102
Figure 6.11: Question 3.4 Results	103
Figure 6.12: Question 3.5 Results	104
Figure 6.13: Question 3.6 Results	105
Figure 6.14: Question 3.7 Results	105
Figure 6.15: Question 3.7a Results	106

List of Acronyms

ACRONYMS	DETAIL
CIA	Confidentiality, Integrity and Availability
ISO	International Organisation for Standardisation
IEC	International Electrotechnical Commission
NIST SP	National Institute of Standards and Technology Special Publication
SANS	SysAdmin, Audit, Network and Security
SETA	Information Security Education, Training and Awareness
SFA	Single Factor Authentication

Chapter 1 : Introduction

This chapter introduces the research study by providing a high-level overview of the study conducted. Information security is introduced as the main field of study, with password security being the key area of study upon which this research study is based.

1.1 Background

Information security is used to protect an organisation's valuable resources such as information, computer hardware and software by preventing unauthorised access, use, disruption, modification and destruction of information (Peltier, 2013). Information is important to the well-being of all organisations and is used for various business decisions. Information is seen as an asset to organisations and therefore their information assets need to be protected against various threats and unauthorised access (McCumber p.44, 2004; Von Solms & Von Solms p.10, 2009).

According to ISO/IEC 27002 (2013), information assets need to be protected from threats. With information assets, there are various threats against the confidentiality, integrity and availability of these assets. Threat sources include external attacks, which are malicious attacks from the Internet through viruses, internal attacks which can come from angry employees, errors made by employees and physical attacks which include theft and natural disasters (Von Solms & Von Solms p.10, 2009). Other threats include worms, Trojan horses, Denial of Service (DoS) attacks and malware. These threats can all cause severe damage to an organisation's information assets and their reputation.

The protection of information and its critical characteristics such as confidentiality, integrity and availability (CIA) need to be ensured to prevent information assets from being compromised. Ensuring the CIA of information involves allowing only authorised users to access the information (confidentiality), ensuring only authorised users may make changes to the information (integrity) and ensuring the information is available to authorised users when required (availability) (Von Solms & Von Solms p.10, 2009). Identification and authentication are commonly used to help ensure the CIA of information assets. This research study focused on the password-based authentication.

Passwords play an important role in our everyday lives as they are used to log into our personal computers, email accounts, bank accounts and also our company computers. Textual passwords are still being used to authenticate users, and remain the most cost-effective and efficient method to control access (Campbell, Ma, & Kleeman, 2011). Passwords act as a protective barrier between a user and their personal and company information. Users should choose the strength of their passwords according to the importance of the information to be protected (McDowell, Hernan, & Rafail, 2009). There are many password policies and standards and best practices that attempt to help users generate secure passwords and maintain their passwords, such as ISO/IEC 27002 (2013), National Institute of Standards and Technology (NIST) and SANS.

If a user's password gets compromised, then the attacker/hacker may have access to the user's personal information such as their banking details, address, and phone number. Having poor and predictable passwords could cause problems such as data breaches and identity theft. A case in point is the Sony data breach which occurred in 2011 where 77 million PlayStation network accounts were compromised. This data breach is viewed as the worst data breach in the gaming community, as it exposed 12 million unencrypted credit card numbers and hackers gained access to full names, passwords, email and home addresses (Armerding, 2017). Another example is, the release of celebrities' private photos, dubbed Celebgate, in 2014. The photos were obtained through a password guessing attack on Apple's iCloud (Cameron, 2014). The Yahoo data breach in 2013, which affected the accounts of 3 billion users, is considered the biggest data breach of the 21st century. The data breach compromised real names, email addresses, dates of birth and telephone numbers of 500 million users (Armerding, 2017).

The following section discusses and presents the problem area that this research aimed to address.

1.2 Problem Area

Most organisations develop password policies with the aim of helping users create and manage their passwords. This, in turn, helps ensure the confidentiality, integrity and availability of the organisation's information (Adams & Sasse, 2003; Zhang-Kennedy, Chiasson, & Oorschot, 2016). Although users generally try to adhere to

password policies, many password policies seem difficult when it comes to adhering to the password length, the password composition requirements and the requirement to change a password after the password has passed the expiration period. The more online accounts users have, the more likely they are to demonstrate poor password behaviour such as password reuse across many accounts and creating simple and predictable passwords (Gaw & Felten, 2006; Stobert & Biddle, 2014).

Password policies that are perceived as too restrictive cause high levels of dissatisfaction for users. Users try to adhere to password policies but often do not follow the prescribed password policy guidelines (Adams & Sasse, 2003; Zhang-Kennedy et al., 2016). Users therefore adopt various coping strategies such as password reuse, password sharing and the writing down of passwords (Inglesant & Sasse, 2010; Stobert & Biddle, 2015).

A negative attitude could negatively influence the way users perceive password policies. The negative attitude could lead to insecure password management behaviours. Research has shown that negative attitudes towards password policies affect behavior with regards to coping strategies (Choong, Theofanos, & Liu, 2014; Shay et al., 2010). A negative attitude is not the only reason why users demonstrate insecure password management behaviours. There are other human factors that play a role such as human memory limitations, apathy, and lack of education, training and awareness. Users might generally be willing to adhere to password policies. However, due to the limitations of human memory they cannot remember all their passwords, which results in them creating, writing down and reusing weak passwords (Choong et al., 2014; Gaw & Felten, 2006). In addition, users might not be educated on the creation and management of passwords, or the importance of passwords, and may need some level of awareness to protect themselves, as they cannot always rely on the system administrator to protect them (Furnell & Clarke, 2012; Helkala, 2011). Users may also exhibit apathy, which decreases the motivation of users to adhere to password policies (Furnell & Thomson, 2009). These human factors impact the ability of users to adhere to password policies and are discussed in detail in Chapter 4.

In order to address these human factors, NIST has proposed new password policy guidelines. These guidelines, will allow for improved password management, make password policies more user-friendly and facilitate adherence to password policies (CISO, 2016). The new guidelines include:

- Passwords are allowed to be up to 64 characters or more in length;
- Accept printing ASCII characters as well as the space character, can be used in a password;
- Newly created and changed passwords must be compared against a list that contains values commonly used or compromised, such as Dictionary words and passwords obtained from previous breaches;
- Systems should not require users to change passwords periodically;
- No composition rules that force the user to use particular characters or a combination of characters (NIST SP 800-63B, 2016).

However, users' perceptions regarding these new NIST password policy guidelines were yet to be determined. This research argues that before organisations implement password guidelines, they need to determine users' perceptions of such guidelines.

The problem identified for this research is stated as:

Organisations often implement password policy guidelines without taking into consideration users' perceptions regarding such guidelines. This could result in users adopting various password management coping strategies.

To address this problem, certain research objectives were identified and are presented in Section 1.3. Section 1.4 presents and discusses the various research methods used and how they relate to the research objectives, while Section 1.5 discusses the delineation and limitations of this research study. Section 1.6 presents the chapter layout of the study, while Section 1.7 provides a list of publications related to this research study. Section 1.8 concludes this chapter.

1.3 Research Objectives

In order to address the identified problem stated in Section 1.2, the primary objective of this study is:

To determine users' perceptions regarding key elements of current password policy guidelines.

The following secondary objectives were identified as necessary in achieving the above-mentioned primary objective:

1. To determine the key elements of current password policy guidelines.
2. To determine human factors and coping strategies relating to password management.
3. To evaluate current password policy guidelines with regard to coping strategies.

Table 1.1 depicts the relation between the research objectives and the research methods used.

RESEARCH OBJECTIVES	METHOD(S) USED
Primary objective: To determine users' perceptions regarding key elements of current password policy guidelines	Literature review Survey (Questionnaire)
Secondary objective 1: To determine the key elements of current password policy guidelines	Literature review Content analysis
Secondary objective 2: To determine human factors and coping strategies relating to password management	Literature review Content analysis Survey (Questionnaire)
Secondary objective 3: To evaluate current password policy guidelines with regard to coping strategies	Literature review Argumentation

Table 1.1: Research Objectives

The secondary objectives were used to meet the primary research objective. The primary research objective of this research was met through literature reviews and a survey in the form of a questionnaire. Secondary objectives 1, 2 and 3 all used literature reviews. However secondary objective 1 also made use of a content analysis, secondary objective 2 made use of a survey and a content analysis and secondary objective 3 made use of argumentation.

The following section discusses the research methods that were used in this research study. Chapter 5 discusses the research design in detail.

1.4 Research Methods

This section presents and discusses the research methods which were used in this research study.

1.4.1 Literature Review

A literature review is used to report on relevant information found in the literature related to a specific field. It is very important to go through all the relevant literature studies with a fine-tooth comb to get all information in the specific field (Olivier p.8, 2009).

This research study consists of three literature review chapters. The first literature review chapter (Chapter 2: Understanding Passwords) aims to provide an understanding of the importance of password security. The second literature review chapter (Chapter 3: Password Policies) presents and discusses the various standards and best practices that relate to password authentication. This chapter also identifies the common elements found in the standards and best practices that should to be included in password policies. The third literature study chapter (Chapter 4: Human Factors Relating to Passwords) aims to determine the human factors relating to password policies and to identify coping strategies that users commonly adopt in trying to adhere to such policies.

1.4.2 Survey

A survey is used to determine the characteristics or opinions of people that one is interested in (Olivier p.78, 2009). According Saunders, Lewis, & Thornhill (2012), a survey can be conducted in the form of a questionnaire or an interview.

Saunders et al p.420., (2012) state that questionnaires are categorised as either self-administered or interview administered. For the purpose of this research study, the self-administered questionnaire, in the form of a web-based questionnaire, was adopted. Further detail regarding the design of the survey and the process undertaken is provided in Chapter 5, Section 5.7.

In order to meet the primary objective, which used the survey, survey objectives were identified, as outlined in Table 1.2 below.

SURVEY OBJECTIVES	
Survey objective 1	To determine users' perceptions towards the Sample Password Policy
Survey objective 2	To determine coping strategies used by users regarding password management
Survey objective 3	To determine users' perceptions towards the new NIST SP 800-63B (2016)

Table 1.2: Survey Objectives

The three survey objectives as seen in Table 1.2 were supported by questions to ensure that objectives were met. The survey questions that are linked to the survey objectives are presented and discussed in Chapter 5, Section 5.8.

1.4.3 Content Analysis

According to Krippendorff (2012), a content analysis “ is a research technique for making replicable and valid inferences from text (or other meaningful matter) to the contexts of their use “. The focus of a content analysis is to provide the researcher with new insights and understandings of phenomena and what that means for the researcher.

This research study used a content analysis in Chapter 2, Section 2.2 in order to identify common themes in existing password literature. This is presented in Chapter 2, Section 2.2. The content analysis also helped to identify the human factors and coping strategies with regard to password management, by focusing on the existing literature that had the themes *password coping strategies* and *human factors*.

1.4.4 Argumentation

Argumentation is the interdisciplinary study of how conclusions can be reached through logical reasoning (Van Eemeren & Grootendorst, 2004). Argumentation combines existing facts to derive new facts and conclusions (Olivier p.105, 2009).

This research study argues that the common elements of password policies affect the human factor limitations and that these limitations force users to adopt insecure coping strategies. These human factor limitations are addressed by NIST SP 800-63B (2016) .This research discusses and argues how NIST addressed the human factors to make adherence to password policies easier. Argumentation was also used to evaluate the standards and best practices with regard to coping strategies.

1.5 Delineation and Limitations

With regards to this research study, certain delineation and limitation boundaries were set.

The scope of this research focused on standards and best practices such as ISO 27002 (2009), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), NIST SP 800-63B (2016) and SANS Password Protection Policy (2014b). These standards were chosen since organisations generally adopt these standards. For example, the South African Reserve Bank has adopted the ISO 27002 standard. This research targeted users in general, including employees in small and large companies, scholars and students within academic institutions.

The following section presents the chapter outline of this research study.

1.6 Chapter Outline

This dissertation consists of eight chapters. This section briefly discusses the contents of these chapters.

Chapter 1- Introduction: This chapter introduces the research study by providing the background literature and problem area of this research. This research aims to address the problem identified in Section 1.2 through various research objectives. Furthermore, the research methods used to meet these objectives, and how they relate to this research study, are discussed. Lastly, the research delineation and limitations, as well as the chapter layout of this dissertation, are presented. The publication related to this research study is listed

Chapter 2 - Understanding Passwords: This chapter provides an overview of the importance of passwords by providing the results of a content analysis of existing password research that was conducted to identify common themes. In addition, the McCumber model is presented and discussed as a security measure to protect an organisation's information assets. This chapter also addresses each of the themes identified from the content analysis such as Password Security and Strength, Password Threats, Password Management Lifecycle, Password Coping Strategies, Human Factors and Alternative Methods.

Chapter 3 – Password Policies: This chapter provides an overview of various password-related standards and best practices. The standards and best practices

which this research focused on were ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2(2013), NIST SP 800-63B (2016) and the SANS Password Protection Policy (2014b). For the purpose of this research study, only certain sections of the standards and best practices deemed to be relevant, were discussed. In addition, this chapter identified common elements of password policies by analysing the various standards and best practices.

Chapter 4 – Human Factors Relating to Passwords: This chapter focuses on identifying the various human factors and how they affect users' password coping strategies. This is done by linking the password policy common elements which were identified in Chapter 3 to the human factors by discussing how certain common elements affect the human factors identified. In addition, this chapter identifies and discusses various password coping strategies that users commonly adopt. Furthermore, the human factors identified are also linked to certain coping strategies. Education, training and awareness programmes are presented as a solution to address the human factors.

Chapter 5 – Research Design: This chapter introduces the research process which was used to conduct this research study. It presents the research approach used in this research study, namely the inductive reasoning approach. In addition, the data collection, respondents, and the survey questionnaire process are presented. Furthermore, the survey design highlights the three survey objectives which were established and how they were linked to specific questions of the survey.

Chapter 6 – Results and Findings: This chapter reports on the general results and findings from the survey. It presents the demographics of the respondents as well as results from the Sample Password Policy and Behaviour and Coping Strategies sections. In addition, this chapter compares the results of employees and the student/scholar groups to determine if there is a correlation between the two.

Chapter 7 – Interpretation and Discussion: This chapter interprets the results from the survey and determines respondents perceptions towards the new NIST SP 800-63B (2016). Furthermore, password policy recommendations were presented based on the respondents perceptions towards the new NIST standard.

Chapter 8 – Conclusion: This chapter concludes the research study by presenting how and where the research objectives were met within the dissertation.

1.7 Related Publications

The following publication relates to this research study. For the full paper refer to Appendix C:

Fredericks, D. T., Fitcher, L. A., & Thomson, K. (2016). Comparing Student Password Knowledge and Behaviour : A Case Study : In *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance* (pp. 167–178) Frankfurt, Germany.

1.8 Conclusion

This chapter provided a brief background to this research study. The problem statement for this research was identified as well as the primary and secondary research objectives which were used to address the identified problem.

The following chapter addresses the importance of password security.

Chapter 2 : Understanding Passwords

The aim of this chapter is to provide an overview of the importance of passwords by providing a content analysis of password research conducted between 2010 and 2016. It also highlights password threats and discusses the password management lifecycle by referring to the various stages of the password management lifecycle. The common elements of password policies are identified. In addition, alternative methods used to replace password-based authentication systems are discussed.

2.1 Introduction

Passwords have been around since ancient Egypt (from around 1600 B.C.E) where they were used to encrypt tombs and artefacts (Bunson, 2014). However, in the context of computers, the first system that had a login command and requested a password from the user, was introduced in 1961 by the Massachusetts Institute of Technology (MIT) (Amendola, 2015; Walden & Van Vleck, 1973). Passwords play an important role in our everyday lives. They are used to log into personal computers, email accounts, bank accounts and company computers. The purpose of passwords is to protect users' personal information and accounts by making sure that only the user has access to his/her information, thereby ensuring the confidentiality of their accounts and information.

Today, an organisation's information is one of its biggest assets and has become a vital part of most organisations by providing value to such companies and organisations. The IT systems that companies and organisations have implemented capture, store and process information. These systems are exposed to a variety of risks, such as data breaches, that compromise the confidentiality, integrity and availability (CIA) of company information (Von Solms & Von Solms p.10, 2009). Companies and organisations need to ensure that their information is protected against possible risks and threats. A threat is a potential cause of an unwanted incident which could result in harm to the system or organisation. A vulnerability is a weakness of an asset that can be exploited by one or more such threats (ISO/IEC 27000, 2012). To protect information, certain controls need to be implemented such as access controls and authentication controls. ISO/IEC 27002 (2013) states that passwords are a form of security authentication and a common way of verifying a user's identity.

This chapter is structured as follows: Section 2.2 discusses the existing password research in the form of a content analysis, followed by sub sections, which discuss each of the themes identified from the content analysis. Section 2.3 concludes this chapter.

2.2 Existing Password Research

Extensive research has been conducted within the password field. For the purpose of this research, a content analysis was conducted in order to establish common themes which relate to passwords. According to Krippendorff (2012), a content analysis “ is a research technique for making replicable and valid inferences from text (or other meaningful matter) to the contexts of their use“. The main focus of a content analysis is to provide the researcher with new insights into and understandings of phenomena and their implications for the researcher. The content analysis, carried out as part of this research study, focused on research studies that were conducted between 2010 and 2017. The content analysis process is explained in more detail in Chapter 5. Table 2.1 lists the password related research of various authors, as well as the common password themes identified during this study. Eight themes were identified, namely: Password Security, Password Strength, Password Threats, Password Management Lifecycle, Password Policy, Password Coping Strategies, Human Factors and Alternative Methods.

LEGEND								
THEME	DESCRIPTION			THEME	DESCRIPTION			
1	Password Security			5	Password Policies			
2	Password Strength			6	Password Coping Strategies			
3	Password Threats			7	Human Factors			
4	Password Management Lifecycle			8	Alternative Methods			
Authors	1	2	3	4	5	6	7	8
Bauer et al (2013)								✓
Bonneau et al (2015)		✓	✓	✓	✓		✓	
Bonneau & Schechter (2014)			✓				✓	✓
Butler & Butler (2015)							✓	
Campbell et al (2011)	✓	✓						
Choong et al (2014)				✓	✓	✓	✓	

Choong (2014)				✓		✓		
Choong & Theofanos (2015)				✓	✓	✓	✓	
Das et al (2014)	✓		✓	✓	✓	✓	✓	
Duggan et al (2012)	✓			✓		✓	✓	
Egelman et al (2013)		✓		✓			✓	
Fahl et al (2013)		✓						
Florêncio et al (2014)	✓		✓		✓			
Florêncio et al (2014b)	✓		✓			✓	✓	
Florencio & Herley (2010)	✓	✓	✓	✓	✓	✓		
Haque et al (2014)			✓	✓	✓	✓	✓	✓
Helkala & Hoddø Bakås (2014)	✓			✓		✓	✓	
Helkala (2011)		✓		✓	✓		✓	
Herley & Van Oorschot (2012)	✓					✓		
Inglesant & Sasse (2010)				✓	✓	✓	✓	
Imperva (2010)						✓		
Lamont (2016)	✓	✓						
Li et al (2014)								✓
Malone & Maher (2011)		✓	✓	✓				
Rastogi & Agrawal (2015)								✓
Renaud et al (2013)		✓	✓				✓	✓
Rouse (2015)				✓				
Sasse et al (2014)			✓				✓	✓
Siciliano (2016)	✓	✓						

Shay et al (2010)			✓	✓	✓	✓	✓	
Simon & Perkins (2016)	✓							
Stobert & Biddle (2014)				✓	✓	✓		
Stobert & Biddle (2015)				✓	✓	✓	✓	
Sun et al (2011)								✓
Tam et al (2010)	✓			✓		✓		
Taneski et al (2014)				✓		✓		
Ur et al (2015)	✓			✓	✓	✓		✓
Ur et al (2016)	✓	✓	✓	✓			✓	
Verizon (2015)	✓	✓						
Von Zezschwitz et al (2013)		✓		✓	✓	✓		
Wash et al (2016)	✓			✓		✓	✓	
Weir et al (2010)		✓	✓	✓	✓			
Zhang-Kennedy et al (2016)	✓		✓	✓	✓	✓	✓	

Table 2.1: Common Password Themes

The following sub-sections discusses each of the themes identified from the content analysis.

2.2.1 Password Security and Strength

The most common and most popular authentication method used for computer-based systems is the textual password. This is due to its simplicity and it being the most cost effective and efficient method to control access to users' information systems (Campbell et al., 2011; Renaud et al., 2013). Users have to remember multiple passwords for their various Apple, Google and Microsoft accounts. The average user has 25 web accounts that require passwords (Florencio & Herley, 2010). The password is one of best authentication methods used as it allows access from anywhere while only needing a simple web browser (Herley & Van Oorschot, 2012).

As mentioned previously passwords act as a protective barrier between the user and their personal or company information. Choosing weak and predictable passwords could have major consequences such as identity theft and data breaches (Siciliano, 2016). In 2014, a total of 79 790 cyber security incidents were reported in 61 countries and 43% of companies in the United States reported a data breach (Verizon, 2015). Examples of companies that were exposed to data breaches include Home Depot (where over 56 million customers' records were leaked) and eBay (which had 145 million records of their customers and employees personal information leaked) (Simon & Perkins, 2016). Data breaches cause both direct and indirect losses. The direct loss involves the emptying of bank accounts and identity theft, whereas the indirect loss includes the time and money involved in securing systems against future security breaches and repairing damage to a company's reputation (Tam et al., 2010). Data breaches can have severe consequences such as the ruining of people's lives, as seen from the Ashley Madison leak in August 2015 (Lamont, 2016).

Password meters can be used to help improve user's password strength, as the password meters give an estimate strength of the passwords (Bonneau et al., 2015). The password strength refers to how strong the password is against cracking tools for example, John the Ripper (Egelman et al., 2013). Numerous studies have been conducted in order to measure the strength of users' passwords. These studies included (Fahl et al., 2013; Helkala, 2011; Malone & Maher, 2011; Ur et al., 2016; Weir et al., 2010). It was found that when users are exposed to password meters, they often choose stronger passwords. However, forcing users to create strong passwords may have drawbacks. For instance, when users are not able to remember their passwords they revert to creating predictable passwords (Egelman et al., 2013).

One way to protect an organisation's information assets is to implement certain controls. Organisations could adopt, for example, the renowned McCumber model, as seen in Figure 2.1, to use as baseline to protect information assets.

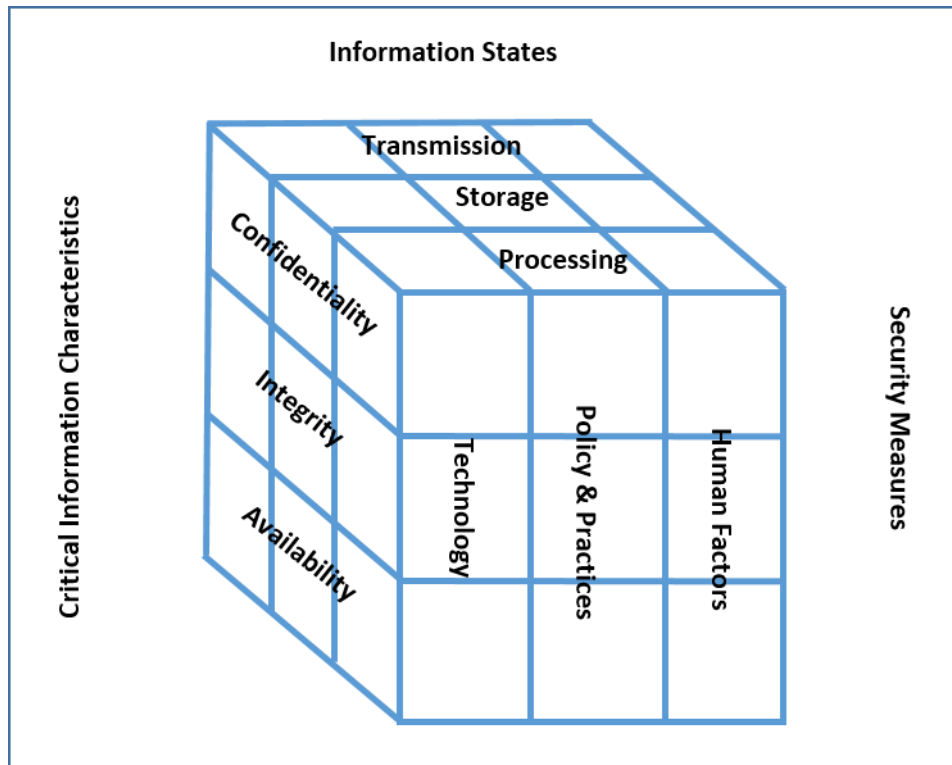


Figure 2.1: McCumber Model (McCumber p.136,2004)

As seen in Figure 2.1, the McCumber model depicts that information has three states, namely transmission, storage and processing and that information has three characteristics, namely confidentiality, integrity and availability. Further, McCumber (2004) states that security measures need to be in place to ensure that the critical information characteristics are maintained while the information moves between states (McCumber p.104, 2004). As seen from Figure 2.1, the security measures include *Technology*, *Policy and Practice* and *Human factors* (originally called Education, Training and Awareness). The *technology* security measure refers to any physical device or technique which is implemented in physical form to ensure that the information characteristics are maintained through any of the information states (McCumber p.105, 2004). An example of a *technology* security measure, is biometric devices. Although the *policy and practices* security measure can help in protecting information, the *human factors* security measure can be seen as the most important security measure, since *technology and policy and practice* must rely on education, training and awareness (McCumber p.106, 2004). This research study does not focus on the *technology* security measure, but rather on the *policy and practice* and *human factors* security measures. The policies and practices are

discussed further in Chapter 3, Section 3.2 and the human factors are addressed in Chapter 4, Section 4.2.

The following section discusses the threats associated with password-based authentication.

2.2.2 Password Threats

Passwords are exposed to various threats such as shoulder surfing, brute force attack, dictionary attacks, shared passwords, and the use of weak passwords, to name a few. Shoulder surfing involves monitoring the user while they authenticate themselves (Renaud et al., 2013), while brute force and dictionary attacks are password cracking methods. Password cracking is the process of guessing or retrieving a password from stored locations or data systems (NIST SP 800-118, 2009). A dictionary attack is an offline attack that takes a known list of words, such as dictionary type words and common passwords, and then compares the list to a password database until a valid password is found (Beaver, 2004; Shay et al., 2010). Brute force, on the other hand, is an offline attack that cracks passwords through trying every combination of numbers, letters and special characters until a password has been found. Brute force is time consuming, depending on the number of accounts being attacked (Beaver, 2004; Herley & Van Oorschot, 2012). Once the password has been cracked, the hacker/attacker has unauthorized access to personal and/or company information.

A further threat to password security, are the users. Users often struggle with the management of passwords. For example, they struggle to create passwords and to remember multiple passwords for multiple online accounts. Users therefore often employ insecure behaviours such as re-using passwords, creating weak passwords, writing down passwords and not changing their passwords (Choong, 2014).

Considering the various password threats, many alternative solutions have been investigated to replace passwords. The following section discusses these alternative methods and indicates the advantages and disadvantages of each authentication method.

2.2.3 Password Management Lifecycle

The password management lifecycle consists of the following three stages generation, maintenance and authentication (Choong, 2014). Figure 2.2 illustrates the three stages of the password management lifecycle. The password management lifecycle was adapted from Choong (2014).

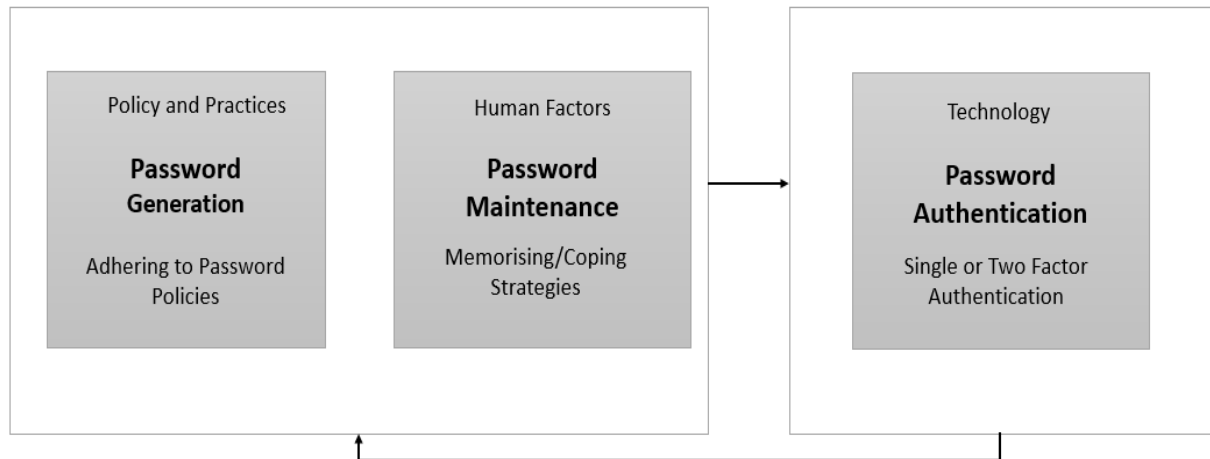


Figure 2.2: Password Management Lifecycle (adapted from (Choong, 2014))

Figure 2.2 depicts the password management lifecycle adapted from Choong (2014). The security measures from the McCumber model also form part of the password management lifecycle. For example, with regard to the Password Generation stage, which links with Policy and Practices, the users would often adhere to password policies when creating passwords for new accounts. The Password Maintenance stage is linked to the human factors, as the users would rely on memorisation or certain coping strategies, such as writing down passwords, in order to keep track of their passwords. The Password Authentication stage links with the Technology security measure, as the users would then authenticate themselves by using either single or two-factor authentication. The sub-sections below discuss each stage of the password management lifecycle.

2.2.3.1 Password Generation

According to Choong (2014), password generation is the first stage of the password management lifecycle. Users have to generate strong and secure passwords based on the password requirements in the related password policy. The stronger the password, the lower the chances of users being hacked and being exposed to malicious software attacks. Password requirements generally consist of rules about

the maximum and minimum password length, use of uppercase and lowercase characters, numbers and special characters (Shay et al., 2010; Taneski et al., 2014). These password requirements help ensure that users are less vulnerable to potential attacks. Online accounts encourage users to create strong passwords by employing an algorithm to determine the strength of strength. Figures 2.3, 2.4 and 2.5 show examples of password requirements from Apple, Google and Microsoft respectively.

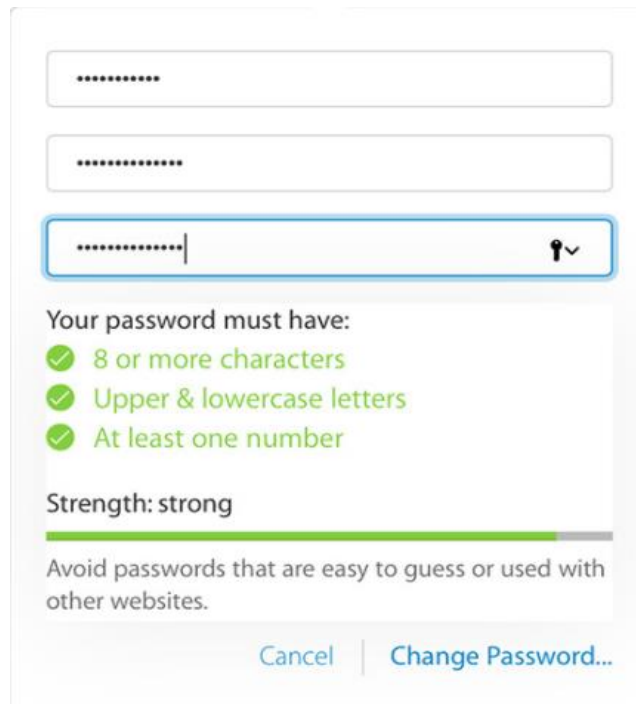


Figure 2.3: Apple Password Requirements (Apple, 2017)

From Figure 2.3, it can be seen that Apple's password-based authentication systems require a user's password to be a minimum of 8 characters, contain upper and lowercase letters and contain at least one number.



Create account

Microsoft account opens a world of benefits.

johnssTarg@gmail.com

Passwords must have at least 8 characters and contain at least two of the following: uppercase letters, lowercase letters, numbers, and symbols.

.....

Figure 2.4: Microsoft Password Requirements (Microsoft, 2017b)

As seen from Figure 2.4, Microsoft requires that passwords must adhere to the following: consist of at least 8 characters, of which at least two must be uppercase letters, lowercase letters, numbers or symbols.

Create your Google Account

Just is all you need

gets you into everything Google.



Get it all with
... and pick up

Password strength:

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. [Why?](#)

Name

First

Last

You can't leave this empty.

Choose your username

@gmail.com

You can't leave this empty.

Create a password

|

Confirm your password

Birthday

Figure 2.5: Google Password Requirements (Google, 2017b)

Figure 2.5 requires Google account passwords to be at least 8 characters in length and not to use a password from another site or something that might be obvious to potential hackers, such as a pet's name.

It is clear that there are commonalities between the three online accounts (Apple, Microsoft and Google) with regard to their password requirements. They all have a minimum password length and the password complexity rule, which requires the user to choose a password that contains uppercase and lowercase characters, numbers and special characters. These commonalities are referred to as common elements of password policies and are discussed further in Chapter 3, Section 3.3.

2.2.3.2 Password Maintenance

According to Choong (2014), password maintenance is the second stage of the password management lifecycle, which takes effect after the password has been generated for the specific account. Once the password has been created, the user makes decisions about how they will keep track of the password. The user can choose to either memorise or store the password with the aid of some mechanism. If the user decides to memorise the password, s/he needs to apply some strategies to ensure that the password gets encoded in his/her long term memory. Examples of strategies used for memorising a password include: using mnemonic systems, rote rehearsing and typing the password multiple times to remember it. If users decide to store their passwords, they need to decide on the storage mechanism, such as writing the passwords down or storing the passwords in files. Users can make use of password managers to store passwords if they have many passwords that they utilise. Although password policies usually stipulate, "Do not write down your password", the ISO/IEC 27002 (2013) states that users can write down their passwords or save it in a software file, as long as it is stored securely and the method of storing adheres to the password policy.

2.2.3.3 Password Authentication

According to Choong (2014), password authentication is the last stage of the password management lifecycle where the password is used to gain access to the specific account or system. This stage is repetitive, as the password will be utilised multiple times to gain access until the password is changed (due to either being forgotten, expiration of the password or the password being compromised).

Although the use of passwords helps to protect information assets, it is still not enough to prevent unauthorised access. A further authentication method needs to be implemented, such as a single or two-factor authentication method. Single factor authentication (SFA) secures access to a network or website by identifying the party requesting access through one category of credentials (Rouse, 2015). An example of SFA is a password. Two-factor authentication adds an extra layer of protection against anyone trying to seek unauthorised access (Leal, 2017). Banking systems make use of two-factor authentication. For example, when a user signs into an account with the appropriate password, a verification code is sent to the user's phone if s/he wants to perform a financial transaction. The system uses the verification code as a secondary authentication method. The user will not be able to perform the financial transaction without entering the verification code.

By considering these two authentication methods, it becomes evident that two-factor authentication is the better option, as it provides better security of information. Passwords are not enough to provide full protection. Many organisations are turning to two-factor authentication because of the value of their information assets and the severity of attacks (Leal, 2017). To further emphasise the importance of two-factor authentication, ISO/IEC 27002 (2013) Section 11.1.2 states that two-factor authentication controls need to be implemented where confidential information is restricted to only authorised users.

2.2.4 Password Policies

With regard to password policies some authors (Bonneau et al., 2015; Choong & Theofanos, 2015; Shay et al., 2010; Zhang-Kennedy et al., 2016) highlighted the importance of password policies and how they are they used to generate and maintain password and prevent users from selecting passwords that are easier to crack. Zhang-Kennedy et al. (2016) aimed to determine various aspects of password policies. Password policies consist of technical and user perspective (non-technical) aspects. The technical aspects include making sure that passwords are not stored in plain text, are encrypted, and that users get meaningful feedback when entering the incorrect password. This research study will focus on the user perspective (non-technical) aspect.

In the content analysis, it was determined from the studies that password policies consisted of certain commonalities, namely: Password Length, Password Complexity, Password Expiration, Password History and Password Protection (Choong & Theofanos, 2015; Das et al., 2014; Inglesant & Sasse, 2010; Shen, Yu, Xu, Yang, & Guan, 2016). These commonalities are referred to as the common password policies and are defined as follows:

- **Password Length** - refers to the minimum and maximum number of characters of a password. For example, 8 characters in length,
- **Password Complexity** - refers to the requirement that users formulate strong passwords that include upper and lower case characters, alphanumeric and special characters in a password,
- **Password Expiration** - refers to the maximum length of time users can keep their passwords before they have to change it,
- **Password History** - refers to the limit on how often users can reuse the same password for the account,
- **Password Protection** - refers to recommendations to protect users' passwords, such as not sharing passwords with people and not attaching passwords in email.

This theme is discussed in more detail in Chapter 3: Password Policies

2.2.5 Password Coping Strategies

With regard to password coping strategies, various authors (Choong and Theofanos (2015); Choong et al (2014); Inglesant & Sasse (2010) and Stobert and Biddle (2015)) aimed to determine users' password coping strategies with respect to password policies. They found that when users generated new passwords, they often used the Re-using Passwords and Creating Weak Passwords coping strategy and to keep track of their passwords, the coping strategy used was the writing down of passwords. Other studies by Das et al (2014); Helkala & Hoddø Bakås (2014); Shen et al (2016); Wash et al (2016) aimed to determine which coping strategies users generally adopt. The users' coping strategies included Re-using Passwords, Writing Down Passwords, Not Changing Passwords and Creating Weak Passwords.

This theme is discussed further in Chapter 4, Section 4.3.

2.2.6 Human Factors

With regard to the human factors theme, various studies have identified that the human memory has a severe impact on users' password management (Bonneau et al., 2015; Butler & Butler, 2015; Choong et al., 2014; Duggan et al., 2012; Shay et al., 2010). Having to remember multiple passwords puts a strain on the human memory, and due to the human memory, users often begin to develop their own methods to remember passwords. Users tend to find it easier to remember frequently used passwords.

Other studies (Butler & Butler, 2015; Choong et al., 2014) identified that attitude and apathy can affect password management. It was determined that users had negative attitudes towards Password length and Password Complexity, which they considered to be annoying and burdensome. Users who had a negative attitude towards password generation requirements often re-used passwords or re-used passwords by making minor changes. The users who found password requirements to be burdensome would write down passwords instead of relying on memorisation. The lack of motivation to apply secure password practices led users to create weak passwords, re-use passwords, write down and not change passwords. It can be seen that the human factors often force users to adopt coping strategies.

Helkala (2011) and Helkala & Hoddø Bakås (2014) mention that a lack of education affect users' password management. It was found that users who initially created weak passwords, created stronger passwords after receiving password education. Education, training and awareness are used to address the human factors in Chapter 4, Section 4.4

The human factors theme is discussed in more detail in Chapter 4, Sections 4.2 and 4.3.

2.2.7 Alternative Methods

This section refers to the *technology* security measure of the McCumber model and discusses some technologies that can be used to replace passwords. Over the years, many alternative solutions to replace passwords, such as smart cards, graphical passwords, biometrics, password managers and Single Sign-On solutions, have been considered (Haque et al., 2014; Renaud et al., 2013; Ur et al.,

2015). However, these alternative solutions have both advantages and disadvantages, as discussed in this section.

The smart card is a card, the same size as a credit card that is used to authenticate the user (Abie, 2006). It is the most popular method of providing two factor authentication. An example would be systems that use a password as a form of single authentication and then use the smart card to authenticate users, thus providing the second-factor authentication. Smart cards can be used to reduce human memory problems (Adams & Sasse, 2003). However, smart cards must be kept close at hand and can be lost, stolen or shared and can be broken easily (Abie, 2006).

Graphical passwords allow the user to select images in a specific order. The sequence of images is used as a password alternative (Rouse, 2014). Graphical passwords address the human lack of ability to remember a large number of passwords for many accounts (Renaud et al., 2013). Graphical passwords, however, are prone to shoulder surfing and require more storage space than textual passwords (Pathak, 2013). An example of the graphical password would be the Microsoft Windows 8 picture passwords.

Biometrics are an authentication method that identifies a user based on unique physiological traits such as fingerprints, iris scans and retina scans or behavioural characteristics, which use voice recognition or keystroke scans. The use of biometrics prevents users from sharing passwords and forgetting them (Abie, 2006). However, biometrics are more expensive to implement than textual passwords and if biometric data is compromised, it is often harder to replace (Schneier, 2015).

Password managers consist of a database which stores a user's password for all their accounts (Li et al., 2014). While password managers reduce the difficulty of remembering multiple passwords, all the user's credentials are reliant on the strength of the master password. One of the biggest vulnerabilities of password managers is that an attacker/hacker can steal all the passwords of a user if the master password is compromised (Bonneau & Schechter, 2014; Li et al., 2014). Examples of password managers include Lastpass and Roboform.

Single Sign-On is a user authentication service that allows the user to use one set of user login credentials to access multiple applications such as, Facebook Login,

Microsoft Login and Google Login (Rouse, 2016). The Single Sign-On begins with a user being enrolled with an identity provider such as Facebook, Microsoft or Google. When a user logs into a service provider that uses the identity provider, the identity provider sends a set of attributes about the user to the service provider for example age, gender, email address, location and friend list (Rastogi & Agrawal, 2015). This presents a privacy issue for the user as they do not know which information the identity provider sends. In addition, users wish to be informed as to which information is being used and who it is being shared with (Bauer et al., 2013; Haque et al., 2014). Based on all the information that is being used by the service provider, it can be understood why users have trust, security and privacy concerns with Single Sign-On (Sun et al, 2011).

2.3 Conclusion

This chapter highlighted the importance of passwords. Most systems are still using passwords as it still remains the most cost-effective and most efficient method to control access to information assets. This chapter discussed existing password related research and identified key themes that are highlighted in current research. These included Password Security, Password Strength, Password Attacks, Password Lifecycle, Password Policy, Password Management Behaviours and Human factors. Each of the themes identified from the content analysis was discussed in detail. For example, password threats were discussed and, as a result, some alternative methods to replace passwords were examined by presenting the advantages and disadvantages of each. The password management lifecycle from creating a new password to maintaining that password, was also discussed. The common elements of password policies, namely Password Length, Password Complexity, Password Expiration, Password History and Password Protection, were identified within the password policies theme. The Password coping strategies and human factors were discussed briefly as these are discussed in more detail in Chapter 4.

In this chapter, the McCumber model was introduced as a control to protect information assets. The security measures from the McCumber included technology, policy and practice and human factors. As stated earlier, the researcher will not focus on the technology security measure. McCumber (p.105,2004) states that relying on technology is not enough and that other security measures need to

be in place, such as policies and practices and human factors. Passwords need to adhere to certain password requirements, which is achieved through a password policy.

In conclusion, there are a number of challenges with passwords. Textual passwords have been used over a long period of time and are still being used to authenticate users today. Although other alternative authentication methods have been investigated, many systems still revert to using textual passwords as it remains the most dominant, most cost-effective and most efficient means by which to authenticate and control access (Butler & Butler, 2015; Zhao & Yue, 2014).

The following chapter discusses password policies, as well as the standards and best practices that organisations commonly use when developing their organisational password policies.

Chapter 3 : Password Policies

The aim of this chapter is to provide an overview of password policy guidelines. Various standards and best practices concerning the common elements of password policies were analysed and discussed.

3.1 Introduction

The previous chapter highlighted the importance of password security. It also discussed the McCumber model, which can be used to protect information assets. This chapter focuses on the *Policy and Practice* security measure from this model. In doing so, it discusses password policies that organisations adopt as well as the standards and best practices commonly used as guidelines to implement password policies. A policy is designed to inform all employees within the organisation of how they should behave in relation a specific topic (Killmeyer p.78, 2006)

Relying on technology as a security measure is not enough to protect information. In. this regard, password policies also need to be implemented. The enforcement of policies, such as password policies, aids in protecting information (McCumber p.105, 2004). Password policies are rules that are used to improve computer security by providing guidelines to create stronger passwords, to change user passwords after a certain number of days and to better protect user passwords. A password policy is designed to protect organisational resources such as their information assets. Password policies are aimed at protecting the confidentiality, integrity and availability (CIA) of the organisation's information, and are therefore key in protecting such information. Password policies are aimed at ensuring good password behaviours from the users (Choong & Theofanos, 2015). User passwords need to adhere to the password policies that organisations create. Organisations use various standards and best practices as guidelines to develop their password policies.

The following section discusses password policy standards and best practices, including ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), NIST SP 800-63B (2016) and the SANS Password Protection Policy (2014b). 'Best practices' refers to ISO/IEC 27002 (2013) and 'standards' refer to NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), NIST SP 800-63B (2016) and

SANS Password Protection Policy (2014b). Section 3.3 discusses the common elements found across various password policy standards and best practices. Section 3.4 discusses the structure of password policies and Section 3.5 concludes this chapter.

3.2 Password Policy Standards and Best Practices

Standards consist of a specific set of rules, procedures or conventions that are agreed upon between parties in order for them to operate more uniformly (Killmeyer p78, 2006). This implies that the standards set a level of expectation with respect to how employees complete their work responsibilities. A best practice provides a reference to help organisations in assessing their security risks and implementing the appropriate security controls (Von Solms & Von Solms p.20, 2009).

For the purpose of this research, the researcher focused on the following international standards and best practices, namely ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), NIST SP 800-63B (2016) and SANS Password Protection Policy (2014b). These specific standards and best practices were chosen because they focus on the guidelines of password policies and many organisations rely on standards and best practices when developing their password policies. These are discussed in the following sub-sections.

3.2.1 ISO/IEC 27002

The ISO/IEC 27002 (2013) *Information technology - Security techniques - Code of practice for information security controls* is an international standard that provides best practice recommendations. It is designed for organisations to use as a reference or as a guideline document for implementing commonly accepted information security controls (ISO/IEC 27002, 2013). The standard allows organisations to implement commonly accepted information security controls and to develop their own information security management guidelines. Both the private and the public sector can use this standard. An example of an organisation that adopts the ISO/IEC 27002 (2013), is the South African Reserve Bank. For the purpose of this research, the following sections of the standard were considered to be relevant.

Section 9.3.1 of the ISO/IEC 27002 (2013) document, which discusses the use of secret authentication information, states that:

- a) users should be advised to keep their passwords confidential and not to reveal their passwords to anyone, including people of authority;
- b) users should avoid keeping a record of passwords on paper, software file or hand-held devices unless the password can be stored securely and the method of storing adheres to password policy;
- c) users must change passwords immediately when the password has been compromised;
- d) passwords must have a sufficient minimum length; be easy to remember; not be based on anything somebody else could easily guess; not be obtained using personal information (for example, names, numbers, dates of birth etc); not be vulnerable to dictionary attacks; not be made up of all numeric or all-alphabetic characters; temporary passwords must be changed at first log-on;
- e) users must not share users passwords;
- f) users must ensure proper protection of passwords;
- g) users must not use the same password for business and non-business purposes (preventing password reuse).

This section of the standard also mentions that organisations can make use of Single Sign-On (SSO) or other alternative authentication methods, for example biometrics, to reduce the number of passwords that users have to remember and protect, thus making alternative authentication methods such as biometrics more appealing.

Section 9.4.2 discusses the “Secure Log on Procedures” and states that computer systems should:

- a) not display system or application identifiers until the log-on process has been successfully completed;
- b) display a general notice warning that computers should only be accessed by authorised users;
- c) not provide help messages during the log-on procedure that could aid an unauthorised user;
- d) validate the log-on information only on completion of all input data;
- e) protect against brute-force log-on attempts;
- f) log unsuccessful and successful attempts;

- g) raise a security event if an attempted or successful breach of log-on controls is detected;
- h) display the information on completion of a successful log-on such as date and time of the previous successful log-on and details of any unsuccessful log-on attempts since the last successful log-on;
- i) not display passwords being entered;
- j) not transmit passwords in clear text over a network;
- k) terminate inactive sessions after a defined period of inactivity then re-authenticate the user ; and
- l) restrict connection times to provide additional security for high-risk applications and to reduce the window of opportunity for unauthorised access.

Section 9.4.3 of the standard, which discusses password management systems, states that password-based authentication systems should:

- a) maintain accountability by enforcing the use of individual user IDs and passwords;
- b) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
- c) enforce a choice of quality passwords;
- d) force users to change their temporary passwords at the first log-on;
- e) force regular password changes as needed,for example, force the user to change their password after a certain number of days;
- f) maintain a record of previously used passwords and prevent password reuse;
- g) not display passwords on the screen when being entered
- h) store password files separately from application systems; and
- i) store and transmit passwords in protected form (encryption).

The ISO/IEC 27002 (2013) has further technical aspects of password-based authentication systems. For example, Section 12.4.1 “Logging and Monitoring” states that records of successful and rejected system access attempts need to be logged.

Table 3.1 below depicts what were identified in the ISO/IEC 27002 (2013) as common elements in password policies.

COMMON ELEMENTS	DETAIL
Password Length	Passwords must have a sufficient minimum length.
Password Complexity	Passwords must not be all numeric or all- alphabetic characters. Passwords must not be vulnerable to dictionary attacks and not be based on anything somebody else could easily guess.
Password Expiration	Password-based authentication systems should enforce regular password changes as needed
Password History	Password-based authentication systems should maintain a record of previously used passwords and prevent password reuse
Password Protection	Users should be advised to keep their passwords confidential and not to reveal their passwords to anyone, including people of authority. Users must change passwords immediately when the password has been compromised

Table 3.1: ISO/IEC 27002 Common Elements

Table 3.1 depicts what ISO/IEC 27002 (2013) states about password requirements, as well as what the password-based authentication systems should require. These common elements could be used as a baseline for organisations in developing password policies.

The following sub-section discusses NIST SP 800-118 (2009), which is now a retired standard; however, it is still important as it discusses requirements by password management systems, as well as recommendations to better protect users' passwords, which are still relevant today.

3.2.2 NIST SP 800-118

The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines. NIST provides renowned standards that many organisations adopt. The NIST SP 800-118 (2009) *Guide to Enterprise Password Management*, guides organisations by providing recommendations for password management, which involves implementing and maintaining password policies (NIST SP 800-118, 2009). Effective password management could mitigate the risk of compromising password-based authentication systems. The purpose of this standard is to assist organisations in understanding common threats against character-based password authentication systems and how to mitigate such threats. For the purpose of this research only those sections deemed to be relevant to this study are discussed.

In Section 2 it was stated that organisations should review their Password Policy periodically as major technology changes could impact existing policies. Policy makers need to take this statement into consideration when implementing the organisation's password policy as there may also be new standards and best practices that have updated their guidelines, such as NIST SP 800-63B (2016). Section 3.2.3, which discusses password strength, states that having strong passwords helps mitigate password guessing and cracking. A strong password is determined by a password's length and its complexity. An example of password complexity is the requirement that characters from at least three of the following four groups be present in the password: lowercase letters, uppercase letters, numbers and symbols. This section also mentions that it may be helpful for organisations to set policies that make passwords easier to remember, such as favouring longer passwords over more complex passwords. If a user's password is weak, the user is often forced to create a different password. A less stringent solution is to educate users on password strength requirements and also to run password cracks against their stored passwords in order to identify weak passwords.

Section 3.4, which discusses Password Expiration, suggests that a user must be forced to create a new password after a certain number of days. This section states that password expiration is often a source of frustration for users, who are required to create and remember new passwords. Therefore, organisations should consider the password expiration period, and balance it against security needs and usability. Password-based authentication systems should remind users that their passwords will expire. This section also states that the password expiration will not be effective if users use their old password when having to change their passwords. A way to prevent users from using an old password is by keeping track of passwords, which is called Password History. Password History keeps the passwords or password hashes and then compares it against the new password or password hash. Password History only works on single authentication methods and not on multiple authentication methods.

With regard to the technical aspects of password-based authentication systems, the NIST SP 800-118 standard has a few guidelines. Section 3.2.3 states that password-based authentication systems should limit the number of authentication attempts and that passwords should be encrypted. Section 4 mentions that

organisations can use Single Sign-On as an alternative authentication method. Table 3.2 below depicts the common elements identified in the NIST SP 800-118 (2009).

COMMON ELEMENTS	DETAILS
Password Length	A strong password is determined by a password's length and its complexity. For example, Password Length is often set as a range, such as permitting passwords from 8 to 15 characters long.
Password Complexity	A strong password is determined by a password's length and its complexity. An example of Password Complexity is to require that characters from at least three of the following four groups be present in every password: lowercase letters, uppercase letters, digits, and symbols
Password Expiration	Organisations should decide whether or not to use password expiration and what expiration period to set based on balancing security needs and usability
Password History	Password-based authentication systems should prevent users from reusing previous passwords. One way to prevent this is by password history, which keeps a record of previously used passwords.
Password Protection	User training that stresses the importance of proper password management and protection and explains the risks of password reuse should also be implemented.

Table 3.2: NIST SP 800-118 Common Elements

Table 3.2 depicts what NIST SP 800-118 (2009) states about password requirements, as well as what the password-based authentication systems should require. These common elements could be used as a baseline for organisations in developing password policies.

The following section discusses the new NIST SP 800-63-2 (2013).

3.2.3 NIST SP 800-63-2

The NIST SP 800-63-2 (2013) Electronic Authentication Guideline provides technical guidelines for Federal agencies that implement electronic authentication. According to NIST, electronic authentication is the process of establishing confidence in user identities electronically presented to an information system. For the purpose of this research, only those sections deemed to be relevant to this study are discussed in this section.

Section 6 discusses *Tokens*, also referred to as passwords, within the electronic authentication context. Tokens are possessed by a claimant and controlled through one or more authentication factors (something you know, have, or are). 'Something

you know’ refers to a password, a smart card is ‘something you have’ and a biometric refers to ‘something you are’. Tokens are of various types. For the purpose of this study, the focus is on the memorised secret tokens, which are more commonly known as passwords. Section 6.2.1 states that imposing password complexity rules may reduce the likelihood of a successful guessing attack.

Section 6.3.1.1 discusses the password requirements, as well as password-based authentication system requirements. Table 3.3 depicts the requirements for passwords, as well as password verifiers. A ‘verifier’ is defined as an entity that verifies the user’s identity by verifying the user’s password with the aid of an authentication protocol. The verifier may also need to validate credentials that link the password and identity (NIST SP 800-63-2, 2013). The term ‘verifiers’ refers to password-based authentication systems.

LEVEL	PASSWORD REQUIREMENTS	VERIFIER REQUIREMENTS
Single-factor	Passwords must be a minimum of 6 characters or more. Chosen from alphabet of 90 characters.	Limit the number of failed authentication attempts an attacker can make
Two-factor	Passwords must be a minimum of 8 characters or more. Chosen from alphabet of 90 characters. Password must have composition rules.	Limit the number of failed authentication attempts an attacker can make.

Table 3.3: NIST SP 800- 63-2 Password and Verifier Requirements

Table 3.3 depicts the different password requirements for each level of authentication. The single-factor authentication requires passwords to be a minimum of 6 characters or more, chosen from an alphabet of 90 characters, whereas the two-factor authentication requires passwords to be a minimum of 8 characters or more, chosen from an alphabet of 90 characters. Two-factor authentication requires that passwords also include composition rules. With regard to the verifier requirements, the verifier refers to the password-based authentication system and requires that there must be a limit on the number of failed authentication attempts an attacker can make.

Section 7.1.2 suggests that password-based authentication systems may require users to change their passwords after the passwords have passed their expiration period. This standard also has some technical guidelines related to aspects of password-based authentication systems. Only those aspects deemed to be relevant are discussed. As seen from Table 3.3, the verifiers require that there is a limit on

the number of failed authentication attempts. Both sections 7.3.1.1 and 7.3.1.2 state that passwords must not be stored in plaintext, but should be encrypted. Section 7.3.1.2 states that passwords must be hashed.

Table 3.4 below depicts the common elements identified through the NIST SP 800-63-2 (2013).

COMMON ELEMENTS	DETAILS
Password Length	Passwords must be a minimum of 6 characters for single-factor authentication and a minimum of 8 characters for two-factor authentication
Password Complexity	Passwords need to have composition requirements for two-factor authentication.
Password Expiration	Password-based authentication systems may require users to change their passwords after they have passed their expiration period
Password History	The standard does not say anything about keeping a record of previous passwords.
Password Protection	To prevent password threats, users should not share passwords with others or write their passwords down

Table 3.4: NIST SP 800-63-2 Common Elements

Table 3.4 depicts the common elements found in the NIST SP 800-63-2 (2013). For example, with regard to the Password Length it states that for single-factor authentication the passwords need to be a minimum of 6 characters or more, whereas for two-factor authentication it requires that passwords be a minimum of 8 or more characters. Password Complexity is only required through two-factor authentication. Password-based authentication systems may require users to change their passwords after the expiration period.

The following sub-section discusses the new NIST SP 800-63B (2016) which replaces the NIST SP 800-63-2 (2013).

3.2.4 NIST SP 800-63B

The DRAFT NIST SP 800-63B (2016) *Digital Identity guide - Authentication and lifecycle management* is a new standard created by NIST. This standard can be used by governmental organisations as well as non-governmental organisations, on a voluntary basis. The standard provides technical guidelines to organisations for the implementation of digital authentication (NIST SP 800-63B, 2016). This standard replaces the previous standard, NIST SP 800-63-2 (2013). As seen from sub-section 3.2.3, there were certain requirements for passwords, as well as password-

based authentication systems, within the NIST SP 800-63-2 (2013). For the purpose of this research, only those sections of the NIST SP 800-63B (2016) deemed relevant to this study, are discussed.

Section 5.1.1.2, which discusses the requirements specifically needed for password-based authentication systems, mentions that:

- password-based authentication shall require users' passwords to be a minimum of 8 characters and that systems should allow passwords at 64 characters or more in length,
- password-based authentication systems must allow printable ASCII characters, as well as the space character and emoji's,
- password-based authentication systems shall not store a "hint" that is accessible to an unauthenticated user and also not prompt users to provide specific types of information to users such as "What was the name of your first pet?" when creating passwords;
- password-based authentication systems shall compare new and changed passwords against a list of commonly-used, expected or compromised passwords. The list may include: passwords obtained from previous breaches, dictionary words, repetitive characters and context-specific words such as the name of the service and username. If the chosen password is found in the list, then the system must notify the user that they need to create a different password and provide a reason for the rejection of the password;
- password-based authentication systems should not impose composition rules;
- password-based authentication systems should not require users to change their passwords periodically. However, systems shall force a change if there is evidence of compromise.
- password-based authentication systems should offer an option to display the password (rather than a series of dots or asterisks) until it is entered.

NIST SP 800-63B (2016) discusses some technical aspects of password-based systems as well as usability considerations in Section 10.1:

- password-based authentication systems must store passwords in a form that is resistant to offline attacks;

- passwords must be hashed with a salt value using an approved hash function;
- password-based authentication systems should offer an option to display the password being entered to help with memorising the password;
- password-based authentication systems should provide meaningful error messages and state how many attempts the user has left;
- password-based authentication systems should allow a minimum of 10 attempts to enter a password; and
- password-based authentication systems should force the user to re-authenticate themselves in the case of user inactivity.

Table 3.5 below depicts the common elements identified in the NIST SP 800-63B (2016).

COMMON ELEMENTS	DETAIL
Password Length	Memorized secrets (passwords) SHALL be at least 8 characters in length, if chosen by the user. Verifiers SHOULD permit user-chosen memorised secrets of at least 64 characters or more in length.
Password Complexity	Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorised secrets.
Password Expiration	Verifiers SHOULD NOT require memorised secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.
Password History	Does not say anything about password history in this standard
Password Protection	Change passwords if they have been compromised. Passwords must not be based on personal information. Password-based authentication systems must provide meaningful error messages.

Table 3.5: NIST SP 800-63B Common Elements

From Table 3.5 it can be seen that password-based authentication systems would no longer force users to change their passwords periodically or force them to use composition requirements in their passwords. The Password Complexity, Password Expiration and Password History elements have changed from previous standards and best practices. By changing these specific elements, the standard is trying to make adherence to password policies easier for the user.

The following section discusses the SANS Password Protection Policy (2014b).

3.2.5 SANS Password Protection Policy

The SANS Password Protection Policy (2014b) is a standard created by the SANS Institute for the Internet community. This policy can be used freely by organisations and there is no prior approval required (SANS, 2014b). The purpose of this policy is to establish a standard for the creation of strong passwords, the frequency of changing passwords and the protection of passwords.

Section 4.1, which discusses password generation, states that all passwords must conform to the SANS *Password Construction Guidelines*. These guidelines require, passwords to consist of at least 12 alphanumeric characters; contain both upper and lowercase letters; contain at least one number; and contain at least one special character (SANS, 2014a). A further password generation tip is that users must not use the same password for company accounts and other non-company accounts. In addition, users must not use the same password for various company access needs.

Section 4.2 discusses Password Maintenance as follows:

- Section 4.2.1, which discusses Password Maintenance, states that all system-level passwords (administration accounts) must be changed at least on a quarterly basis.
- Section 4.2.2 states that all user-level passwords (email, web, desktop) must be changed at least every six months. However, the recommended change interval is 4 months.
- Section 4.2.3 mentions that password cracking or guessing should be performed on a periodic or random basis by the Information Security Team. If the password is guessed or cracked during the process, then the user must be required to change the password using the password construction guidelines, as recommended.

Section 4.3, Password Protection, mentions some recommendations users need to take into consideration to better protect their passwords:

- Section 4.3.1 states that passwords must not be shared with anyone and must be treated as sensitive and confidential information;

- Section 4.3.2 states that passwords must not be inserted into email messages or other forms of electronic communication;
- Section 4.3.3 states that passwords must not be revealed over the phone;
- Section 4.3.4 states that passwords should not be revealed on questionnaires or security forms;
- Section 4.3.5 states that systems should not hint at the format of a password (for example, my family name);
- Section 4.3.6 states that users must not share company passwords with anyone, including administrative assistants, secretaries, managers, etc;
- Section 4.3.7 states that users should not write their passwords down and store them anywhere in their office and not to store passwords in a file, on a computer system or mobile devices.;
- Section 4.3.8 states that users must not use the “Remember Password” feature of applications (for example, web browsers);
- Section 4.3.9 states that any user suspecting that his/her password may have been compromised, must report the incident and change all passwords immediately;

The SANS Password Protection Policy (2014b) discusses a few technical aspects of password-based authentication systems. For example, Section 4.4, Application Development, states that passwords must not be stored in clear text, nor transmitted in clear text over networks.

Table 3.6 depicts the common elements identified in the SANS Password Protection Policy (2014b) and SANS Password Construction Guidelines (2014a).

COMMON ELEMENTS	DETAIL
Password Length	Contain at least 12 alphanumeric characters.
Password Complexity	Contain at least one number, contain both upper and lower case letters and contain at least on special character.
Password Expiration	All user-level passwords must be changed every six months.
Password History	Does not say anything about keeping a record of previously used passwords but states user must not use business passwords for non-business accounts.
Password Protection	Passwords must not be shared with anyone. Passwords must not be inserted into email messages. Do not hint at the format of a password.

Table 3.6: SANS Common Elements

Table 3.6 presents the SANS Password Protection Policy (2014b) common elements identified through the standard. With regard to the password length the standard states that passwords should be a minimum of 12 alphanumeric characters and requires passwords to contain at least one of the following: one number, uppercase and lowercase letters and special characters for password complexity. SANS requires passwords to be changed every six months and gives more recommendations to further protect their passwords, such as not sharing passwords and not inserting passwords in an email.

The following section discusses the common elements identified from the standards and the best practices referred to in this chapter.

3.3 Summary of Common Elements

From the previous section, which discussed various password policy standards and best practices, the common password policy elements were listed from each standard and best practice. Table 3.7 depicts the common elements identified in the various standards and best practices studied. However, Table 3.7 does not include the technical aspects of password-based authentication systems as this study focuses on non-technical aspects.

COMMON ELEMENTS	STANDARDS AND BEST PRACTICES				
	ISO/IEC 27002 (2013)	NIST SP 800-118 (2009)	NIST SP 800-63-2 (2013)	NIST SP 800-63B (2016)	SANS Password Protection Policy (2014b)
Password Length	✓	✓	✓	✓	✓
Password Complexity	✓	✓	✓		✓
Password Expiration	✓	✓	✓		✓
Password History	✓	✓			
Password Protection	✓	✓	✓	✓	✓

Table 3.7: Common Elements of Password Policies

Table 3.7 depicts the common elements identified across the five standards, namely: ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), NIST SP 800-63B (2016) and the SANS Password Protection Policy (2014b). NIST SP 8000-63B (2016) does not include Password Expiration,

Password Complexity and Password History. The reason why these common elements do not feature in this standard is stated in Section 5.1.1.2 of the NIST SP 800-63B (2016). Passwords do not need to be changed periodically, but rather by users' own choice or if the password has been compromised. Many organisations implement the Password Expiration with the aim of reducing the potential impact of unauthorised use of a password. However, it is often a source of frustration to users, as they have to create and remember new passwords periodically (ISO/IEC 27002, 2013). It could be argued that the reason this guideline was not included in the new standard, is due to the usability issue users had with Password Expiration.

NIST SP 800-63B also states that password-based authentication systems do not need to impose composition rules. Although Password Complexity mitigates the risk of password guessing attacks, it also makes the passwords harder for the users to remember. As a result, users tend to adopt coping strategies such as writing the password down. NIST considered this a motivation for favouring longer passwords over complex passwords. This is evident from Section 3.2.3 of NIST SP 800-118 (2009), which states that organisations should set easier password policies, such as favouring longer passwords over complex passwords. Password-based authentication systems should accept passwords that are up to 64 characters or longer, which is stated in Section 5.1.1.2 of NIST SP 800-63B (2016). This standard does not mention anything about Password History since users are not required to change their passwords periodically.

Both NIST SP 800-118 (2009) and SANS Password Protection Policy (2014b) state that password guessing or cracking may be performed against stored passwords to identify weak passwords on a random basis or periodically. NIST SP 800-63B (2016) changes this rule and states that passwords must be checked against a list of commonly breached, compromised passwords when users create or change a password. The process of checking the password is done when users create a password. This process will reduce the acceptance of weak passwords and lower the chances of users' passwords being compromised.

It is important for policy makers within organisations to make informed decisions when creating or revising their password policies. Policy makers should keep in

mind that the password policies must be determined according to the organisation's needs.

A comparison between the previous NIST standards and the new NIST standard needs to be done in order to correlate the differences between them. Table 3.8 depicts the differences between the old NIST standards and the new NIST standard.

COMMON ELEMENTS	NIST STANDARDS		
	NIST SP 800-118 (2009)	NIST SP 800-63-2 (2013)	NIST SP 800-63B (2016)
Password Length	A strong password is determined by Password Length and Password Complexity and requires a set range	Minimum of 6-8 characters	Minimum of 8 with a maximum of up to 64 characters.
Password Complexity	A strong password is determined by Password Length and Password Complexity	Password must contain composition rules	No composition rules
Password Expiration	Password must be changed after expiration period	Password must be changed after expiration period	No password expiration
Password History	Keep a record of previously used passwords	Does not say anything about keeping a record of previously used passwords	Does not say anything about keeping a record of previously used passwords
Password Protection	Proper user training needs to be done on password management and protection	Users should not share passwords with others or write their passwords down	Passwords must not be based on personal information. Check passwords against list of commonly used, compromised passwords

Table 3.8: Comparison Between Various NIST Standards

Table 3.8 compares the old NIST standards to the new standard. The differences in Table 3.8 include:

- Password-based authentication systems allowing 64 characters or more in length, which allows for passphrases;
- Password-based authentication systems not forcing users to abide by complexity requirements;

- Password-based authentication systems not forcing users to change their passwords periodically;
- Password-based authentication systems not keeping a record of previously used passwords; and
- Password-based authentication systems checking users' potential passwords against a list of commonly used or compromised passwords before users have to commit to it.

There are other guidelines that are in the NIST SP 800-63B (2016) that were not in the NIST SP 800-63-2 (2013) and NIST SP 800-118 (2009), such as checking users' passwords against a list of commonly compromised passwords and rejecting the user's password if a match is found.

The following section discusses the structure and content of password policies.

3.4 Password Policy Guideline Implementation

The previous sections discussed password standards and best practices commonly adopted, as well as identified the common elements that are found in the standards and best practices. Now that the common elements have been identified, how does a policy maker use these guidelines to develop a password policy?

In order to determine the structure of a password policy, a number of password policy templates are available which can be used as a baseline to create an organisational/business password policy. With regard to what should be included in the password policy, policy makers should take into consideration the guidelines from the password standards and best practices, as well as the common elements.

The structure of password policies typically includes overview, purpose, scope and policy, which is sub-divided into Password Generation, Password Maintenance and Password Recommendations. With regard to what is included in the password policies, the common elements included are: Password Length, Password Expiration, Password Complexity, Password Protection and Password History. For the Password Generation section, elements included in this section are Password Length, Password Complexity and Password History. For the Password Maintenance section, the elements include the Password Expiration and for the

Password Recommendations section, the elements include the Password Protection element. Refer to Appendix A2 to see the Sample Password Policy.

COMMON ELEMENTS	Microsoft (2017c)	Apple (2017)	Google (2017a)
Password Length	Minimum of 8 characters	Minimum of 8 characters	Minimum of 8 characters
Password Complexity	Must contain characters from three of the following: uppercase and lowercase letters, numbers, special characters	Must contain uppercase and lowercase letters and one number. Can also add extra characters	Use a mix of alphanumeric characters such as uppercase and lowercase letters, numbers and special characters.
Password Expiration	Set between 30 and 90 days depending on the environment	Does not force password to be changed.	Does not force passwords to be changed
Password History	Enforce password history to 24 passwords	Does not state anything	Does not state anything
Password Protection	Strong passwords that are changed regularly reduce the likelihood of successful attacks.	Do not share Apple ID with other people; Set up two-factor authentication for your Apple ID to add an extra layer of security to the Apple ID.	Do not reuse passwords; Do not display passwords on notes; Consider getting a password manager if remembering passwords becomes a problem.

Table 3.9: Microsoft, Apple and Google Password Policies

With regards to Table 3.9, Microsoft, Apple and Google all state that the Password Length should be a minimum of 8 characters. However, none of them state anything with regard to the maximum Password Length. For the Password Complexity they all stipulate that passwords should contain uppercase and lowercase letters, numbers and special characters. Apple does not force passwords to have special characters, although users can use them. Microsoft states that for the Password Expiration, passwords should be changed every 30 to 90 days, whereas Apple and Google do not force users to change their passwords, but allow users to change their passwords by their own choice. With regard to the Password History, Apple and Google do not say anything about keeping a record of previously used passwords. However, Microsoft enforces password history to 24 passwords. This

means that a user must have used 24 unique passwords before they can re-use an old password (Microsoft, 2017c). Apple and Google all give various Password Protection recommendations such as not sharing passwords, not re-using passwords and changing passwords to reduce the likelihood of successful attacks.

3.5 Conclusion

The importance of this chapter was to evaluate the common elements of password policy guidelines by focusing on password standards and best practices. Various standards and best practices were discussed including ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013) and SANS Password Protection Policy (2014b). These are all commonly used by organisations as a guideline or reference when formulating password policies. This chapter also discussed the new NIST SP 800-63B (2016).

It is important that organisations have proper password policies in place, which are set according to an organisation's needs and to protect an organisation's information assets (Microsoft, 2017a). This ensures that only authorised users have access to their information, thus also ensuring the availability of the information. Organisations can make use of these standards and best practices as guidelines when developing their password policies. Organisational policy makers, who create the password policies, need to make sure that the password policies have the common elements Password Length, Password Expiration, Password Complexity, Password History and Password Protection. The common elements should also correlate with the password management lifecycle phases of Password Generation and Password Maintenance. The Password Length, Password History and Password Complexity refer to the Password Generation phase, whereas Password Expiration and Password Protection refer to the Password Maintenance phase.

If policy makers decided to use the NIST SP 800-63B (2016) as a guideline, then the guidelines for some of the common elements namely, Password Expiration, Password Complexity and Password History, have changed because these elements caused usability problems. By removing these specific elements, the standard is trying to make it easier for the user to adhere to password policies, while still being secure. However, it is important that organisations/businesses do not blindly adopt new standards and best practices. Policy makers need to understand

users' perceptions towards new standards and best practices. Further, policy makers need to understand the importance of the standards and best practices, as the password policies needs to align with the organisation's needs and must be secure and usable for the user.

This chapter focused on the *Policy and Practice* security measure of the McCumber model. The following chapter will address the *Human Factor* security measure of the McCumber model by addressing users' coping strategies and human factors relating to password management, as well as evaluating password policy guidelines with regard to coping strategies.

Chapter 4 : Human Factors Relating to Passwords

This chapter focuses on the Human Factor security measure from the McCumber model. The aim of this chapter is to determine the human factors relating to passwords and how the common elements of password policies, identified in Chapter 2, Section 2.2.4, could affect the human factors. Furthermore, this chapter identifies and discusses the coping strategies users commonly adopt and how the human factors affect these coping strategies. Standards and best practices are evaluated to determine how they try and prevent the adoption of insecure coping strategies regarding passwords.

4.1 Introduction

The previous chapter addressed the *Policy and Practice* security measure of the McCumber model, including password policies, standards and best practices. Various password standards and best practices such as NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), ISO/IEC 27002 (2013), NIST SP 800-63B (2016) and SANS Password Protection Policy (2014b) were consulted in order to evaluate the common elements related to password policies. This chapter focuses on the *Human Factor* security measure of the McCumber model by discussing the problems users experience with regard to passwords, as well as by determining the human factors and coping strategies related to password policies.

Many extensive studies have been conducted to understand users' behaviour towards passwords. One of the earliest studies, conducted by Morris and Thompson (1979), discovered that textual passwords are a weak point in an information system's security and that most users' passwords were weak and contained only lowercase letters, numbers or were dictionary words. From the content analysis outlined in Chapter 2, it is evident that many studies were conducted to determine users' password coping strategies, as well as the associated human factors related to passwords. Examples of studies include Stobert and Biddle (2014), who conducted a study on users' behaviour in managing passwords and confirmed that users write down and reuse passwords. This was in line with earlier research which found that users often engage in poor password coping strategies, such as writing down and sharing passwords, thus indicating that users are willing to sacrifice security for convenience (Tam et al., 2010). A recent study conducted by Taneski,

Hericko and Brumen (2014) aimed to determine whether there had been any changes since the Morris and Thompson study in 1979. From the 2014 study it was identified that the same poor practices, such as writing down passwords, creating weak passwords and reusing passwords, were still being used to cope with password management.

This chapter is structured as follows: Section 4.2 addresses the various human factors that relate to passwords, while Section 4.3 discusses users' coping strategies in relation to passwords. Section 4.4 presents the use of education, training and awareness to address the human factors and the coping strategies adopted by users. Section 4.5 evaluates the standards and best practices with regard to users' coping strategies by identifying how they attempt to prevent certain coping strategies and Section 4.6 concludes this chapter.

The following section identifies and discusses the human factors pertaining to passwords and how the common elements of password policies could affect the human factors.

4.2 Key Human Factors

Many users might be willing to adhere to password policies and the password guidelines provided. However, willingness does not necessarily translate into acceptable password-related behaviour. For example, a user may write a password down because it is difficult to remember. Therefore, users may resort to these 'coping strategies' to create, manage and maintain passwords that adhere to password policies. The key human factors addressed by this research includes human memory, attitude and apathy, as discussed in Sections 4.2.1 and 4.2.2 respectively.

4.2.1 Human Memory

Baddeley (p.9,1997) states that the human memory "is a system for storing and retrieving information that is acquired through senses". There are different types of memory, which include sensory, visual and auditory memory. This study focuses more on visual memory as users use visual memory to store and retrieve their passwords. Research has shown that, on average, users have 25 accounts which require passwords and may reuse each password across 6.5 sites (Florencio & Herley, 2010). This could create memorability issues for users, as they have to

remember these passwords for each account. Users often struggle to adhere to the guidelines of password policies because of the huge demand on users' memory. For example, users have to remember passwords and which system and username are associated with it. In addition, users have to remember whether they have changed a password and remember what the new password has been changed to (Sasse, Brostoff, & Weirich, 2001). Sasse, Brostoff and Weirich (2001) state that memorability is the primary user characteristic that impacts password generation and that the important issues related to passwords are the following:

- The capacity of a user's working memory is limited, therefore remembering a certain number of passwords may be problematic;
- User memory decays which means that a user might not remember a password or remember it inaccurately;
- User memory finds it easier to recognise familiar passwords;
- Frequently recalled items are easier to remember than the infrequently recalled ones, therefore frequently typed passwords are easier to remember;
- The retrieval of frequently recalled passwords becomes an automatic process for a user, and;
- Passwords that are meaningful to the user are easier for them to recall.

As a result of these memorability issues pertaining to passwords, it can be identified that users will, most likely, choose passwords that have meaning to them, will choose frequently used passwords over creating new ones, choose easier passwords to remember and writing passwords down.

The password-related standards and best practices attempt to address issues surrounding the human memory. For example, the ISO/IEC 27002 (2013) states that passwords must have a sufficient minimum length which is easy to remember. NIST SP 800-118 (2009) mentions the use of mnemonic methods, altered passphrases, as well as combined and altered words, to create passwords that are strong and easy to remember. The SANS Password Protection Policy (2014b) mentions that users can use passphrases as passwords to make the password easier to remember. NIST SP 800-63B (2016) suggests that password-based authentications

should accept 64 characters or more. This will allow for users to use passphrases as passwords, which could make the password easier for the user to remember.

This chapter links the common password policy elements to the human factors, which could help to explain the insecure coping strategies practiced by users. The common elements of password policies that affect the human memory include the Password Length, Password Complexity, Password Expiration, Password History and Password Protection.

4.2.1.1 Password Length and Complexity

Password Length and Password Complexity require passwords to be of a minimum length and to have a combination of uppercase and lowercase letters, numbers and special characters. These elements make passwords long and harder to crack by attackers. However, users find the passwords difficult to remember (Adams & Sasse, 2003; Bonneau & Schechter, 2014; Morris & Thompson, 1979). Chapter 3, Section 3.4 depicted the different password policies used from Microsoft, Apple and Google. The three organisations do not specify a maximum Password Length. Microsoft mentions, according to best practice, that a minimum of 8 characters is recommended for Password Length because it provides adequate security and is still short enough for users to remember (Microsoft, 2017c). The minimum of 8 characters for Password Length links to NIST SP 800-63-2 (2013) and the new NIST SP 800-63B (2016) standard.

The ISO/IEC 27002 (2013) states that passwords must have a sufficient minimum length, must be easy to remember and must not contain all numeric or all alphabetic characters. The SANS Password Protection Policy (2014b) states that passwords must be at least 12 alphanumeric characters in length and should contain at least one number, both upper and lowercase characters and at least one special character. NIST SP 800-118 (2009) states that it may be helpful for organisations to set policies that make passwords easier to remember.

4.2.1.2 Password Expiration

Password Expiration affects the users' memory. Password-based authentication systems require users to change passwords after the expiration period. As a result, users have to remember new passwords for multiple accounts, which reduces memorability (Adams & Sasse, 2003). As shown in Section 3.4 of Chapter 3, Apple

and Google do not force users to change their passwords, but allow users to change them by their own choice. Microsoft, on the other hand, states that passwords must be changed every 30 to 90 days. Apple and Google's Password Expiration are linked to the new NIST SP 800-63B (2016) standard, which recommends that password-based authentication systems should not force users to change their passwords periodically.

ISO/IEC 27002 (2013) states that password-based authentication systems should force regular password changes as needed. NIST SP 800-118 (2009) realises that Password Expiration is a burden on the users' memory as they have to create and remember new passwords at regular intervals. NIST SP 800-63-2 (2013) states that systems may require users to change their passwords and the SANS Password Protection Policy (2014b) states that user-level passwords must be changed every six months.

4.2.1.3 Password History

Password History prevents users from using previous passwords. This common element also reduces the memorability of passwords, as users cannot reuse old, but perhaps more memorable, passwords and are forced to create new passwords. In Chapter 3, Section 3.4 it was shown that Apple and Google do not keep a record of previously used passwords but do state that users should not reuse passwords, whereas Microsoft keeps a record of users' previously used passwords. Apple and Google's Password History link to the new NIST SP 800-63B (2016) standard, as NIST does not keep a record of users previously used passwords.

The ISO/IEC 27002 (2013) states that password-based authentication systems must maintain a record of previously used passwords which will prevent password reuse. Similarly, NIST SP 800-118 (2009) states that password-based authentication systems should prevent users from reusing passwords by keeping a record of previously used passwords.

4.2.1.4 Password Protection

Password Protection gives the users recommendations on how to further protect their passwords and online accounts. Password policies often recommend that users should not write their passwords down. However, users cannot remember all their passwords, which leads them to writing down their passwords (Duggan et al.,

2012). In Chapter 3, Section 3.4, it was shown that Microsoft, Apple and Google provide some level of protection, such as not to reuse passwords, not to share passwords and to change passwords regularly to reduce successful attacks.

ISO/IEC 27002 (2013) states that Single Sign-On or other alternative authentication methods such as biometrics, can be used to reduce the number of passwords that users have to remember and protect. The SANS Password Protection Policy (2014b) states that passwords must not be shared with anyone and that users should not write down their passwords. NIST SP 800-63B (2016) states that, to help better protect accounts, passwords must not be based on personal information.

The following sub-section discusses the human factors attitude and apathy and how the common elements of password policies affect them.

4.2.2 Attitude and Apathy

Attitude relates to what one thinks and feels towards someone or something in a way that reflects positive or negative attitudes, while behaviour refers to how people act or behave based on their attitude (Semin & Fiedler, 1996). Ajzen and Fishbein (1977) argue that a person's attitude towards an object influences the response to the object and does not predict any given action (behaviour). However, from their study it was discovered that a person's attitude has a strong relation to behaviour when directed at the same target and when it involves the same action. Other research has shown that people's attitudes can influence and even predict certain behaviours (Kraus, 1995).

Further research has shown that apathy plays a role in users' attitudes towards password policies. In terms of information security, apathy is when users are aware of their role in protecting information assets, but are not motivated to do so and do not adhere to good information security practices (Furnell & Thomson, 2009). It could be argued that some users display apathy and are not motivated to adhere to password policies

The sub-sections below illustrates how certain common password policy elements could affect the attitude and apathy of users.

4.2.2.1 Password Length and Complexity

Users often struggle to comply with the Password Length and Password Complexity requirements, as the users' could feel burdened or annoyed towards these specific elements (Choong & Theofanos, 2015; Weir et al., 2010). If users' attitudes are opposed towards the Password Length and Password Complexity requirements, it plays a role in how users create passwords, as their attitude could affect their behaviour. With regard to the Password Complexity element, users are often not motivated to create stronger passwords, but instead create predictable passwords such as putting an "!" at the end and replacing letters with special characters (Ur et al., 2015).

NIST SP 800-118 (2009) states that users create weak and predictable passwords and that a solution would be to educate users on password strength requirements.

4.2.2.2 Password Expiration

With regard to Password Expiration, users often find this element to be rather frustrating and burdensome as they have to keep on creating and remembering new passwords (Das et al., 2014). NIST SP 800-118 (2009) states that users find the Password Expiration frustrating, as they are required to create and remember a new password every few months. With regard to Password Expiration, users are often not motivated and they engage in insecure behaviours, such as not changing passwords and writing down their passwords. Users often engage in these behaviours as they do not foresee any negative consequences for themselves (Simon & Perkins, 2016).

NIST SP 800-118 (2009) states that Password Expiration is a source of frustration for users, as they have to keep on creating unique new passwords. This standard states that organisations should consider their Password Expiration period and balance it with the security needs and usability.

4.2.2.3 Password History

The Password History element prevents users from reusing old passwords, which may cause frustration for users. However, users may still reuse old passwords across accounts (Stobert & Biddle, 2015). As mentioned previously, ISO/IEC 27002 (2013) and NIST SP 800-118 (2009) are the only standard and best practice, respectively, to prescribe that password-based authentication systems should

maintain a record of previously used passwords. A record of previously used passwords would prevent users from reusing passwords and could cause frustration, as users often would reuse passwords when they create new passwords.

4.2.2.4 Password Protection

Password Protection could be affected by apathy on the part of users as users are often not motivated to behave in a secure manner (Adams & Sasse, 2003; Butler & Butler, 2015). With regard to the common elements of password policies, the users are often not motivated to be secure. This lack of motivation could lead users to adopt insecure coping strategies, such as reusing passwords, not changing their passwords, creating weak passwords, writing down passwords and sharing passwords (Butler & Butler, 2015; Tam et al., 2010). ISO/IEC 27002 (2013) states that all employees within an organisation must be motivated to fulfil the information security policies. Organisations need to make sure that their employees are motivated to adhere to information security policies, including password policies.

The password-related standards and best practices address human memory more than they address users' attitude and apathy. One of the ways to address users' attitude, apathy and motivation in password security is through education, training and awareness programmes. This is discussed in Section 4.5.

The following section identifies and discusses the coping strategies users adopt with regard to passwords management.

4.3 Password Coping Strategies

As a result of the limitations related to human factors, as discussed in the previous section, users are often forced to adopt certain coping strategies to help with the password management lifecycle and the adherence to password policies. This section identifies and discusses the coping strategies that users commonly adopt when dealing with passwords.

Two early studies by Tam, Glassman and Vandenwauver (2010), (a web based-survey and an experiment) addressed password management issues for two types of accounts, namely: email and online banking. The survey targeted university students who were asked to list their positive and negative thoughts on the following five password management behaviours:

- choosing a password for the first time,
- changing a password,
- letting someone else use their password,
- taping their passwords next to their computer, and
- sharing their password with friends and family.

From the survey, it was discovered that users could distinguish between strong and weak passwords when they were asked to write down a computer password they considered to be strong. The second study, which was the experiment, was based on the results from the survey in the first study. It examined how the users favour convenience over security and how it impacts password quality. The experiment showed that users share their passwords with friends and family and tape their passwords next to their computers to make password management more convenient. The respondents from the study understood password quality and the negative consequences of bad password management behaviour and yet were willing to trade security for convenience when creating a password.

Users engage in these behaviours because they do not foresee any immediate negative consequences for themselves. Research has shown that people affected by the trauma of data breaches have aspects of their behaviour modified (Simon & Perkins, 2016). A study conducted by Simon and Perkins (2016) discovered that people who experienced no data breaches/hacks had higher levels of trust, while those who had experienced data breaches/hacks, had higher levels of distrust and took actions to protect themselves from future harm. It could be argued that many users will only change their behaviour once they have experienced a traumatic data breach or an identity theft.

Furthermore, studies have shown that users generate weak passwords that are predictable, such as putting digits and symbols at the end of the password and capital letters at the beginning of the password, even for important online accounts (Fahl et al., 2013; Malone & Maher, 2011; Von Zezschwitz et al., 2013). Many users view passwords as a burden, struggle in the management of passwords and exhibit insecure behaviours when in the password generation and password maintenance stages of the password management lifecycle (Duggan et al., 2012; Gaw & Felten,

2006; Stobert & Biddle, 2014). The coping strategies that users commonly adopt include (Inglesant & Sasse, 2010; Stobert & Biddle, 2015):

- Reusing passwords;
- Writing down passwords;
- Creating weak passwords;
- Not changing passwords;
- Using Password managers and Single Sign-On

4.3.1 Reusing Passwords

Password reuse is a coping strategy for managing passwords and occurs due to the demands on human memory. Users often reuse passwords that are complex and reuse passwords that they frequently enter (Wash et al., 2016). The more passwords a user has, the more difficult it is to remember all of them. Infrequently used passwords are also difficult to remember (Sasse et al., 2014; Vu et al., 2007). It was discovered that a user's most used password was typically used across an average of 9 different websites (Wash et al., 2016).

The human factors such as human memory, attitude and apathy can affect users' coping strategies such as the reusing passwords. Users reuse passwords to cope with the difficulty of having to remember multiple passwords across multiple accounts (Ur et al., 2015). Users generally reuse passwords because they consider the Password Complexity and Password Length elements to be burdensome and annoying. Therefore, users adopt password reuse in order to adhere to the password policy.

Various studies have been conducted in order to determine users' password coping strategies. It was determined that reusing passwords was the most common used coping strategy. A study conducted by Shay et al. (2010) targeted university staff and students and aimed to determine the user's attitude towards new password policy requirements. The new password requirements included:

- Passwords would be required to contain at least 8 characters,

- Passwords must include at least one uppercase and lowercase letter, one digit and one symbol,
- New passwords must be checked against dictionary attacks, and
- Passwords containing four or more occurrences of the same character would be rejected.

It was discovered that users found the new requirements annoying, but believed they provided security, while some users struggled to comply with the new password requirements. Inglesant and Sasse (2010) determined which aspects (sections) of the password policy users generally struggle with and what coping strategies users adopt to overcome the problems they have with password policies. The aspects of the password policy which users have trouble with include:

- Changing of passwords (Password Maintenance),
- Creating of passwords (Password Generation),
- Learning of passwords and
- Forgetting a password.

With regard to the coping strategies used to overcome the problem, users commonly choose to reuse passwords. The other coping strategies related to the specific study are presented in the following sub-sections.

In the Shay et al (2010) study, it was discovered that users are more likely to share and reuse their passwords than to write passwords down. Choong, Theofanos, and Liu (2014) studied users' password management behaviours with regard to federal government password policies, in order to develop effective password policies that take into consideration account security and usability. For the Password Generation process, minor changes were made to existing passwords and previous passwords were reused. Employees make use of these coping strategies to try and minimise the need to memorise new passwords as new passwords add to the total number of passwords they have to remember for multiple accounts.

Das et al. (2014) conducted a survey to gain an understanding of users' behaviour and thought processes when they have to create passwords that conform to the password policies for different websites. This study focused on users at universities

that included students and professional staff across several academic departments. It was discovered that when users have to create new passwords, they often reuse an existing password rather than create an entirely new password. The authors investigated further to find out why users reuse passwords and found that when users come across websites with password policy requirements which are difficult to adhere to, they tend to work around the password policy by reusing previous passwords and by making small modifications to their existing one

Haque et al. (2014) wanted to determine how users construct new passwords for websites of different categories. The same password policy was used across the websites, where passwords had to be 6 to 14 characters long with at least one letter and one digit. The websites were classified into five broad categories of account types:

- Identity accounts refer to users' webmail accounts and social networking.
- Financial accounts refer to users' bank accounts.
- Content accounts refer to users' accounts that do not involve significant interactions with other users or financial transactions, for example News sites.
- Sketchy accounts refer to accounts on these sites that are created for superficial purposes and which are often anonymous because users provide a false name or age.
- Shared accounts refer to accounts where the password is shared amongst more than one user, for example a Netflix account.

It was discovered that users reuse passwords less on identity and financial accounts, but would reuse passwords with a slight modification.

Another study conducted by Choong and Theofanos (2015) aimed to determine employees' attitudes towards organisational password policies, as well as coping strategies used the employees. The study found that minor change to existing passwords, using existing passwords and recycling old passwords were commonly adopted during the Password Generation phase. The authors state that employees try to "minimise their effort in generating passwords". Stobert & Biddle (2015)

conducted a study on how computer security experts manage, create and reuse their passwords. With regard to how the subjects created their passwords, it was discovered that their passwords were rarely rejected for failing to comply with password policies, as their passwords included special characters, digits and capital letters. In addition, it was found that password reuse was commonly used among security experts even though this coping strategy is often criticised by security experts.

The password-related standard and best practices attempt to prevent the practice of reusing passwords. ISO/IEC 27002/IEC states that systems must maintain a record of previously used passwords. However, this does not prevent users from reusing passwords from other online accounts. With regard to creating passwords, users often engage in password reuse and recycle old passwords so that they do not struggle to remember their passwords. However, NIST SP 800-118 (2009) prevents users from reusing old passwords by maintaining a record of previously used passwords. The SANS Password Protection Policy (2014b) states that users must not use the same password for company accounts as for non-company accounts. However, users would often still use the same password for work and non-work accounts.

4.3.2 Writing Down Passwords

The writing down of passwords is a coping strategy that refers to users writing down passwords, whether it be on paper or saved in an electronic file. This particular coping strategy is considered to be an insecure password management coping strategy, as it exposes users to risks (Tam et al., 2010). For example, users often write down their passwords on sticky notes and stick them on the computer screen, under the keyboard or other office furniture. Over time, this coping strategy has become more accepted, as can be seen from the international best practice ISO/IEC 27002 (2013), which allows users to write down their passwords, as long as the method of storing the password is secure and adheres to the password policy. An example would be storing the password in a document file that is protected with encryption. Similarly, users could write passwords down on paper and store them securely in a locked location.

With regard to the writing down of passwords on paper or saving it in an electronic file, users make use of this coping strategy to reduce the memory burden of having to remember multiple passwords for multiple accounts (Tam et al., 2010). Users write down their passwords instead of relying on memorisation because they consider the Password Complexity and Password Length to be burdensome (Choong et al., 2014).

In the Inglesant and Sasse (2010) study, the other coping strategy users adopted was the writing down of passwords. The Shay et al. (2010) study (discussed in Section 4.2.2) showed that the users' attitude towards the new password policy was predominantly annoyance. The authors also aimed to determine users' behaviours (coping strategies) under the new password policy. It was discovered that users found it difficult to create passwords with the new password requirements, as some forgot their passwords after creating them. These new password requirements made users more likely to write their passwords down. The Choong, Theofanos, and Liu (2014) study found that, in order for users to keep track of their passwords, the coping strategies users adopted included memorisation, using mnemonics and writing passwords down, whether disguised, stored in a locked location or in plain view. The authors argued that, when users have more information than they can hold in their memory, it is impractical and unreasonable to forbid the use of tools to keep track of such information. It could be argued that this is why ISO/IEC 27002 (2013) has accepted the writing down of passwords, as it would be humanly impossible for those with multiple accounts to remember all their passwords.

Das et al.'s (2014) study found that, in order for users keep track of their passwords, users relied on memorisation, followed by the writing down of passwords. The Choong and Theofanos (2015) study identified that, in order for users to keep track of their passwords, they relied on memorisation, writing passwords down on paper or saving passwords electronically in files. It was found from the study that if users find password requirements burdensome, then they rely more on writing passwords down on paper or saving it electronically, rather than on human memory. In their study, Stobert and Biddle (2015) identified that computer security experts stored their passwords electronically on a computer, while some used password managers. The coping strategies of the security experts were thus found to be similar to that of the ordinary user.

The password-related standard and best practices attempt to prevent the adoption of writing down passwords. Users often write their passwords down on paper or electronic files if the passwords are used infrequently, or if the passwords are long and complex (Adams & Sasse, 2003; Ur et al., 2016). As mentioned previously, it is humanly impossible for users to remember all their passwords due to the limitations of human memory. It can be argued that ISO/IEC 27002 (2013) has taken the human memory limitations into consideration, because they allow passwords to be written down, as long as they are stored securely and the method of storing adheres to the password policy. SANS Password Protection Policy (2014b), in Section 4.3, states that users should not write down passwords.

4.3.3 Creating Weak Passwords

This coping strategy refers to users using dictionary words, common names or other meaningful information to make the password easier to remember (Imperva, 2010; Stobert & Biddle, 2014). Some users do not know what constitutes a secure password, such as randomness and putting uppercase and lowercase letters, digits and symbols in the middle of the password instead of the beginning or the end of a password (Ur et al., 2015). In this regard, password policies often encourage users to not choose weak passwords by forcing passwords to adhere to composition requirements. A further solution is to make users more aware of the security of their passwords with the aid of password meters, which help users to understand the strength of their passwords. Password meters can push users to create more secure passwords. However, pushing users to use stronger passwords may have drawbacks, such as the user not remembering the stronger password or the user may revert to choosing weaker passwords (Egelman et al., 2013).

When users create weak passwords as a coping strategy, they try to make the password easier to remember by using information that is meaningful or important, such as names, dates, predictable words or phrases (Imperva, 2010; Stobert & Biddle, 2014). Having negative attitudes towards password requirements could influence users to create weak passwords as a coping strategy.

Shay et al (2010) identified that when users had to create passwords using the new password policy requirements, they tended to modify old passwords to create new ones and used dictionary words and names to create passwords. From the study, it

can be determined that users found the new password policy annoying and difficult to adhere to. Haque et al (2014) identified that users create weaker passwords for sketchy accounts. From the Choong et al (2015) study it was identified that the employees also adopt the creating of weak passwords in order to do their jobs.

The password-related standard and best practices attempt to prevent the adoption of creating weak passwords by requiring that passwords have a minimum length and contain composition requirements. These include the ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013) and SANS Password Protection Policy (2014b). However, the NIST SP 800-63B (2016) standard does not force users to use composition requirements but by their own choice and allows for the acceptance of passphrases.

4.3.4 Not Changing Passwords

Many users adopt the not changing of passwords coping strategy unless the password-based authentication system forces them to change it. Users often struggle with Password Expiration as they have to create a new password at a set interval (Inglesant & Sasse, 2010). Frequent password changes may cause annoyance and fatigue for users, even though there are security benefits, such as reducing the amount of time an attacker has access to user accounts (Florêncio et al., 2014a; Zhang-Kennedy et al., 2016). However, Zhang, Monroe and Reiter (2010) state that an attacker could still quickly guess the new password. Password Expiration causes a usability issue and is a burden on the users' cognitive processes, as users need to create new passwords after a certain number of days (Herley & Van Oorschot, 2012). This results in users adopting the coping strategy of not changing their passwords. It is understandable that users do not change their passwords, as having to remember multiple passwords for different accounts is burdensome.

The changing of passwords (Password Expiration) causes a usability issue and is a burden on the user's memory (Herley & Van Oorschot, 2012). Therefore, users often do not change the password as a coping strategy. The attitude of users towards the Password Expiration element is frustration as users have to keep changing passwords whenever the password has passed the expiration period (Butler & Butler, 2015; Egelman et al., 2013; ISO/IEC 27002, 2013). Therefore, users often

choose to not change their passwords. With regard to the Inglesant & Sasse (2010) study, it was identified that users do not change their passwords because only 10 passwords from a total of 144 were changed more than once a year.

The password-related standard and best practices attempt to prevent the adoption of not changing passwords coping strategy by forcing users to change their password after the expiration period. ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013) and SANS Password Protection Policy (2014b) all state that passwords must be changed after the expiration period, whereas NIST SP 800-63B (2016) states that password-based authentication should not force users to change their passwords periodically.

4.3.5 Password Managers and Single Sign-On

Password managers are used as a coping strategy to reduce the burden of having to remember multiple passwords (Li et al., 2014). With regard to this coping strategy, it is not as widely employed by users as reusing passwords, writing down of passwords and creating weak passwords. Single Sign-On could be used as a coping strategy when users have the option of using single sign-on instead of logging in with their password. The Single Sign-On login allows the user to use one set of user login credentials to access multiple accounts (Rouse, 2016). Using Single sign-on reduces the number of passwords that users have to remember (ISO/IEC 27002, 2013). Password managers and single sign-on are discussed in detail in Chapter 2, Section 2.5. The use of password manager and Single Sign-On are coping strategies employed by users to avoid having to remember multiple passwords.

Not many users rely on Single Sign-On as a coping strategy. However, some users state that they would want Single Sign-On as the ideal login authentication (Choong et al., 2014). The Inglesant and Sasse (2010) study identified that users preferred Single Sign-On over single password authentication. Das et al. (2014) identified that users also used password managers to keep track of their passwords. Stobert and Biddle (2015) identified that computer security experts also used password managers to keep track of their passwords.

Using Single Sign-On and password managers is not considered an insecure coping strategy, as ISO/IEC 27002 (2013) and NIST SP 800-63B (2016) allow the use of

Single Sign-On. However, none of the standards and best practices mention anything about password managers.

One of the ways to address the human factors relating to passwords management is through education, training and awareness, as discussed in the following section.

4.4 Education, Training and Awareness

Von Solms and Von Solms (p.115,2009) state that employees within an organisation who are required to use a user ID and password to log into any company system, need to be made aware and trained with regard to information security procedures and guidelines. Similarly, ISO/IEC 27002 (2013) states that employees within an organisation should receive some sort of education, training and awareness on information security which is relevant to their job function. One way to achieve this is through an Information Security Education, Training and Awareness (SETA) programme where the aim is to teach employees how to do their jobs securely. The objective of a SETA programme is to make users aware of the importance of, and the need to protect information assets, train users so they will have the necessary skills to do their job securely and educate people so they understand why it is important to protect their information assets (Von Solms & Von Solms p.116, 2009). It is, however, important to distinguish between education, training, awareness.

The aim of an information security awareness programme is to make employees aware of their roles and responsibilities in securing the organisation's information assets (ISO/IEC 27002, 2013). Such an awareness programme needs to be aligned with the organisation's information security policy and can be delivered through campaigns, such as an "information security day" and various media platforms, such as videos, newsletters, posters and the web (ISO/IEC 27002, 2013; NIST SP 800-12, 1995; Von Solms & Von Solms p.116, 2009). However, NIST SP 800-12 (1995) states that an information security awareness programme only addresses the "what" and that it sets the stage for training because employees now recognise and are aware of the importance of security and the need to protect the information assets. Von Solms and Von Solms (p.117,2009) state that having only an information security awareness programme will not suffice, because employees are only aware of the information-related threats and controls. Employees need to be trained to

acquire the necessary skills mitigate threats against the organisations information assets.

The objective of information security training is to teach employees the necessary skills that will allow them to perform their jobs more securely, such as “what” they should do and “how” they should do it (NIST SP 800-12, 1995). According to NIST SP 800-12 (1995), training is most effective when it is targeted to a specific audience. By targeting a specific audience, the training is able to focus on security-related job skills and knowledge that people need when performing their duties. With regard to the specific target audience, there are two types of audiences: general users and those people that require advanced skills (NIST SP 800-12, 1995). General users need to understand good security practices, such as protecting passwords, reporting security violations and incidents and protecting the physical area and equipment. Employees may require more advanced training compared to the basic security practices required by general users. Advanced security training is usually aimed at employees, such as managers, who may need to understand security consequences. This training is more technical than that required for the general user. Training programmes can be delivered through lectures, case studies, workshops and hands-on practice (NIST SP 800-12, 1995; Von Solms & Von Solms p.116, 2009).

Information security education is targeted towards security professionals or employees whose jobs require expertise in security (NIST SP 800-100, 2006; NIST SP 800-12, 1995). Information security education helps employees gain insight and understanding and equips them with the skills needed to ensure the confidentiality, integrity and availability (CIA) of an organisation’s information assets. Such education helps answer the “why” aspect (Amankwa, Loock, & Kritzing, 2014; NIST SP 800-12, 1995). NIST SP 800-12 (1995) states that information security education is usually outside the scope of an organisation’s awareness and training programme, as qualifications for information security education are usually obtained through universities or other graduate institutions.

Without proper information about security education, training and awareness, employees may not be able to do their jobs securely (Von Solms & Von Solms p.116, 2009). With regard to password management, it is an undeniable fact that users

generate weak passwords. It could be argued that users have not received awareness and training on creating and managing passwords (Helkala, 2011). Research has suggested that users who have not been exposed to some sort of awareness programme tend to make up their own rules with regard to passwords (Adams & Sasse, 2003). Furnell (2007) states that users do not use safe password practices due to a lack of knowledge and guidance. This could result in major consequences. To further emphasise the lack of education and guidance on passwords, Helkala and Hoddø Bakås (2014) conducted a study on employees in the Norwegian area and discovered that there is a lack of education and guidance on passwords amongst employees. It can therefore be argued that many organisations do not implement proper password-related education, training and awareness programmes. However, setting up an information security education, training and awareness programme within an organisation is not an easy job and comes with a major constraint, which is cost (NIST SP 800-12, 1995). NIST SP 800-12 (1995) states that the cost consideration for awareness, training and education programmes include:

- The cost of preparing and updating materials
- The cost of providing the programme
- Employee time spent attending the programme or watching the videos
- The cost of outside courses and consultants, which includes travel expenses

Despite the major cost constraint, the SETA programme still provides a positive impact on the organisation in the long run, as employees will be able to do their jobs more securely and know “how” to do it and even understand “why” they are doing it (NIST SP 800-12, 1995; Von Solms & Von Solms p.116, 2009). However, owing to the cost constraint, most small companies will not be able to implement a SETA programme as they do not have the necessary financial means.

The following section evaluates the standards and best practices with regard to how they attempt to lower the adoption of insecure coping strategies related to passwords.

4.5 Conclusion

This chapter focused on the *Human Factor* security measure of the McCumber model. Human factor limitations, such as human memory and attitude and how they affect users' passwords, were discussed. In addition, the chapter explained how certain common elements of password policies affect the human factors. Users' coping strategies with regard to password management such as Reusing Passwords, Writing Down Passwords, Creating Weak Passwords, Not Changing Passwords and Using Single Sign-On and Password Managers were identified. Furthermore, it was identified that human factor limitations often lead the users to adopt certain coping strategies. The human factors play a role in users' adherence to the password policies, for example, users that are not motivated towards password policy rules and requirements often create weak passwords which can easily be compromised. Thus, users need to be motivated to follow the password policy requirements and need to be educated on the consequences of choosing weak passwords (Florêncio et al., 2014; Stobert & Biddle, 2015).

After the coping strategies were identified, the standards and best practices were evaluated with regard to the coping strategies to identify how they attempt to mitigate certain coping strategies. The ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), and SANS Password Protection Policy (2014b) state that the user should not write down their passwords. However, users do still often write down their passwords as a means of coping. It can be identified from the chapter that current standards and best practices, ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013) and SANS Password Protection Policy (2014b), often cause users to adopt various coping strategies. However, the new standard adopted by NIST SP 800-63B (2016) aims to make the password policies more user friendly while still being secure.

As mentioned earlier, the new standard could lower the rate at which users adopt coping strategies. To verify this, users' perceptions towards the new standard need to be determined. This is discussed in Chapter 7.

The following chapter discusses the research design of this research.

Chapter 5 : Research Design

This chapter introduces the research process that was followed when conducting this research study. The aim of this chapter is to provide a brief discussion of the research approach, as well as the research techniques and the data collection process. Lastly, it provides the design of the questionnaire as it relates to the survey objectives.

5.1 Introduction

Chapter 1 presented the research objectives of this study, which need to be achieved in order to address the problem identified. In order to achieve these research objectives, the researcher followed a research process. Section 5.2 of this chapter discusses various research approaches and provides logical reasons as to why the inductive reasoning approach relates to this study. Section 5.3 presents and discusses the research process which was followed, while Section 5.4 highlights the sampling techniques used. Section 5.5 discusses the data collection process used for the survey, which took the form of a questionnaire. Section 5.6 presents the targeted respondents for the survey and Section 5.7 discusses the survey design by presenting the questions which were used to achieve the survey objectives of this research study. Section 5.8 concludes this chapter.

5.2 Research Approach

According to Saunders, Lewis, & Thornhill (2012), there are a number of research approaches that are commonly adopted, including the deductive and inductive approaches. The sub-sections below discuss these research approaches in more detail.

5.2.1 Deductive Reasoning

Deductive reasoning generalises from the general to the specific, which means it starts with a theory which is developed from the researcher's academic literature reading. The data collection is used to evaluate propositions related to an existing theory (Saunders et al. p.144, 2012). For example, the following statements would be deductive, "All men are mortal. Harold is a man. Therefore Harold is mortal". With deductive reasoning, if the premises are true, then the conclusion must be true. Therefore, the conclusion that Harold is mortal, is true (Bradford, 2017) .

5.2.2 Inductive Reasoning

Inductive reasoning occurs when known premises are used to generate untested conclusions (Saunders et al. p.144., 2012). This reasoning generalises from the specific to the general. Data collection is used to explore a phenomenon, identify themes and patterns and create a conceptual framework. According to Saunders et al (2012), researchers using inductive reasoning, work with qualitative data in order to establish different views of phenomena. An example of inductive reasoning is “If a person takes a coin from a bag, and that coin is a penny, and the third coin from the bag is also a penny then all the coins in the bag are pennies”. Even though the premises are true about a penny being a coin, inductive reasoning allows the conclusions to be false (Bradford, 2017).

The research reasoning that was used for this research study was the inductive reasoning approach. This was achieved by collecting data from the existing literature to identify a problem within the information security field. The problem addressed by this research is that ***Organisations often implement password policy guidelines without taking into consideration the users’ perceptions regarding such guidelines. This could result in users adopting various password management coping strategies.*** Once the problem was identified, primary and secondary research objectives were established to address the problem identified. The primary and secondary research objectives can be found in Chapter 1, Section 1.3. Different research methods were used to collect primary and secondary data. Secondary data was collected through literature reviews within the specific field of password security. Primary data was collected by conducting a survey in the form of a questionnaire. Both qualitative and quantitative data was collected through the survey to understand users’ perceptions towards current password policy standards and best practices. From the survey, the respondents’ perceptions towards current password policies were identified.

5.3 Research Process

This section discusses the research process that the researcher has followed in order to address the problem identified.

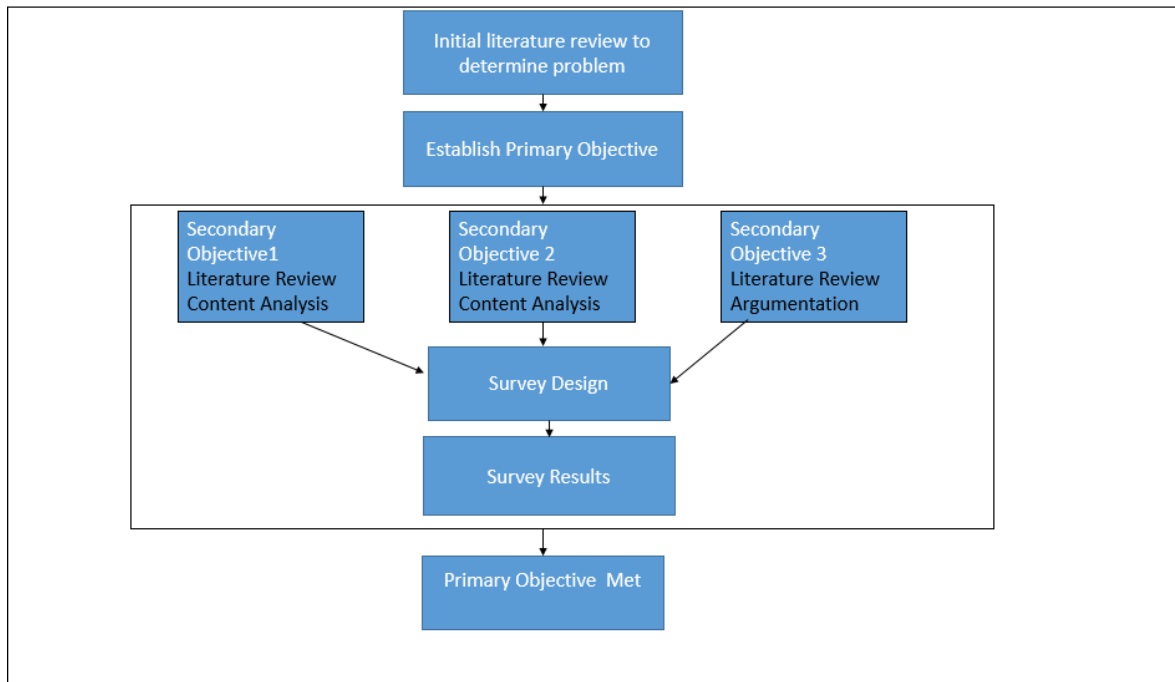


Figure 5.1: Research Process

As depicted in Figure 5.1, an initial literature review was conducted in order to determine a problem in the field of information security, namely password security. Once the problem was identified, a primary research objective was established in order to address the problem, together with secondary objectives to meet the primary objective. The primary objective of this research study was ***To determine users' perceptions regarding key elements of current password policy guidelines.*** The secondary objectives include:

1. To determine the key elements of current password policy guidelines.
2. To determine human factors and coping strategies relating to password management.
3. To evaluate current password policy guidelines with regard to coping strategies.

Figure 5.1 depicts the appropriate research methods that were used to meet each of the secondary objectives identified. In order to achieve secondary objective 1, literature reviews and content analyses were conducted on password-related standards and best practices in order to determine key elements of password policies. In order to achieve secondary objective 2, literature reviews and content analyses were used to determine the human factors and coping strategies relating

to password management. The themes *Human Factors* and *Password Coping Strategies* identified from the content analysis in Chapter 2, Section 2.2, were used to determine the human factors and coping strategies with regard to password management. Once the human factors and coping strategies were identified, it was then determined how the common elements of password policies affect the human factors and how certain human factors could influence users to adopt certain coping strategies. Literature reviews and argumentation were used to achieve secondary objective 3, by evaluating the standards and best practices with regard to coping strategies and how they attempt to prevent users from adopting coping strategies. The survey was designed to determine users' perceptions towards key elements of current password policy guideline, as well as to identify user coping strategies. The literature reviews and content analysis related to the secondary objectives 1,2 and 3 provided valuable input into the design of the questionnaire which is discussed in Section 5.7

The following subsections will address each of the research methods used.

5.3.1 Literature Review

The purpose of a literature review is to report on relevant information found in the literature related to a specific field. It is very important to go through all the relevant literature thoroughly to acquire all the information in the specific field (Olivier p.8, 2009).

Various online databases were used to gather the relevant information on password security, such as ScienceDirect, Elsevier, IEEE Explore Digital Library, Springer and Google Scholar. The main search terms used on the online library databases included: "passwords", "password policy", "user password behaviour", "password management", "password security" and "password coping strategies". The literature review was conducted in order to meet secondary objectives 1, 2, and 3. Secondary objective 1 aimed to determine the key elements of password policy guidelines. Password-related standards and best practices, such as ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), NIST SP800-63B (2016) and SANS Password Protection Policy (2014b), were used to determine the key elements of password policies. Secondary objective 2 aimed to determine human factors and coping strategies relating to password management. This was achieved

by reviewing current relevant literature. Secondary objective 3 aimed to evaluate password policy guidelines with regard to coping strategies. The standards and best practices, ISO/IEC 27002, NIST SP 800-118, NIST SP 800-63-2, NIST SP800-63B (2016) and SANS Password Protection Policy (2014b), were used to identify how they attempt to prevent users from adopting certain coping strategies.

5.3.2 Content Analysis

According to Krippendorff (p.24,2012), a content analysis “is a research technique for making replicable and valid inferences from text (or other meaningful matter) to the contexts of their use“. The focus of a content analysis is to provide the researcher with new insights and understandings of phenomena and what that means for the researcher.

Thematic content analysis refers to one of the forms of content analysis and is the process of identifying common themes in the text for content analysis (Guest, MacQueen, & Namey, 2011). With regard to this research study, thematic content analysis was used to identify themes across various password-related research between the years 2010 and 2016. Chapter 2, Section 2.2, lists the themes identified, such as *Password Policies*, *Password Coping Strategies* and *Human Factors*, to name a few.

Secondary objective 2 used content analysis to determine human factors and coping strategies relating to password management. By using the themes which were identified from the content analysis, it was decided to focus on the existing literature which had the *Password Coping Strategies* and *Human Factors* themes, in order to identify the human factors and user coping strategies with regard to password management.

5.3.3 Argumentation

Argumentation is the interdisciplinary study of how conclusions can be reached through logical reasoning (Van Eemeren & Grootendorst, 2004). Argumentation combines existing facts to derive new facts and conclusions (Olivier p.105, 2009).

This research study argues that common elements of password policies affect human limitations which forces users to adopt insecure coping strategies. This research also uses argumentation by evaluating password-related standards and

best practices in relation to coping strategies and by identifying how they attempt to prevent users from adopting insecure coping strategies.

5.3.4 Survey

A survey is used to determine the characteristics or opinions of people that one is interested in (Olivier p.78, 2009). Surveys come in various forms and are categorised into two groups according to instrumentation and according to the span of time involved. Instrumentation involves the use of a questionnaire or an interview. The self-administered questionnaire is widely used, such as using a web survey, and interviews may be telephonic, face-to-face or online. The span of time involved may be cross-sectional or longitudinal. Cross-sectional surveys ask respondents about a specific topic at a specific point in time, while longitudinal surveys involve the researcher collecting data over a period of time and determining if there are any changes in the data (Sincero, 2012). This research used the questionnaire which is discussed in Section 5.7.

The primary research objective was met through the survey, which determined users' perceptions regarding key elements of current password policy guidelines. Secondary objective 2 was also achieved through the survey where the users' coping strategies were identified.

The following section discusses the sampling technique used for this research study.

5.4 Sampling Techniques

According to Saunders et al (p.260,2012) a researcher would use a sampling technique based on the research objectives. They state that in some cases it may be possible to collect and analyse data from every possible case or group, for example a census. However, for many researchers it will be impossible to collect and analyse all data available as there are restrictions such as time, money, and, often access. Sampling techniques enable the researcher to reduce the amount of data needed by considering the data from a specific sub-group (Saunders et al p.261., 2012). Sampling techniques are divided into two types, namely:

- Probability or representative sampling, and
- Non- probability sampling.

Probability sampling involves the researcher selecting a suitable sample size and making conclusions about a population from the sample. The sample needs to be representative of the population (Saunders et al p.261., 2012). Non-probability samples provide a range of alternative techniques for sampling such as convenience sampling. For the purposes of this research, the non-probability convenience sampling technique was chosen, as the sample is not representative of the population.

Convenience sampling involves selecting a sample because they are easily available and obtainable for the researcher (Saunders et al., 2012). Saunders et al (2012) state that convenience sampling is used widely (for example, Facebook surveys). However, it is typically prone to bias and influences that are beyond one's control. Skowronek & Duerr (2009) state that convenience sampling can generate useful data if steps are taken to control uncertainty and bias, for example, by implementing the following:

- Control and assess the sample's representativeness: involves the researcher attempting to obtain a sample that is a small version of the population
- Diversity: involves the researcher being objective when distributing the questionnaire, by not making judgements about who should be asked to participate in the study.

With regard to convenience sampling, this research study controlled and assessed the sample's representativeness by targeting general users, such as students and staff within academic institutions and employees within small or large companies that use passwords on a regular basis. This was done by providing a URL link on the researcher's Facebook and LinkedIn accounts, which were accessible by such general users. With regard to diversity, the questionnaire did not focus on a specific group, for example, employees in large organisations. Instead, the questionnaire was made diverse by allowing more respondents to answer the questionnaire, such as scholars, students, employees and pensioners. The researcher did not make judgements as to what type of employees, students and pensioners answered the questionnaire. This questionnaire catered to all people that used passwords on a regular basis. Once the type of sampling was chosen, data collection was conducted through the survey.

5.5 Data Collection and Analysis

Data collection can gather primary or secondary data. Primary data is data that is gathered by the researcher first-hand, which involves observing the subject or examining a phenomenon (Driscoll, 2011). The objective of primary data is to learn something new on a subject or a phenomenon, which can be supported by other researchers. Secondary data is obtained through the researcher studying existing literature on a certain subject or phenomenon. The researcher has to make sure that they thoroughly cover the relevant literature (Olivier p.13, 2009).

The questionnaire is the most commonly used primary data collection method, as each respondent is expected to answer the same set of questions. It provides an efficient way of collecting responses (Saunders et al p.416., 2012).

For the purposes of this research, both primary data and secondary data were collected. The secondary data was gathered through reviewing existing literature within the password security field. The objective of the literature review was to determine the key elements of password policy guidelines, to determine human factors and coping strategies relating to password policies, and to evaluate password policy guidelines with regard to coping strategies. The primary data was gathered through the survey, in the form of a questionnaire.

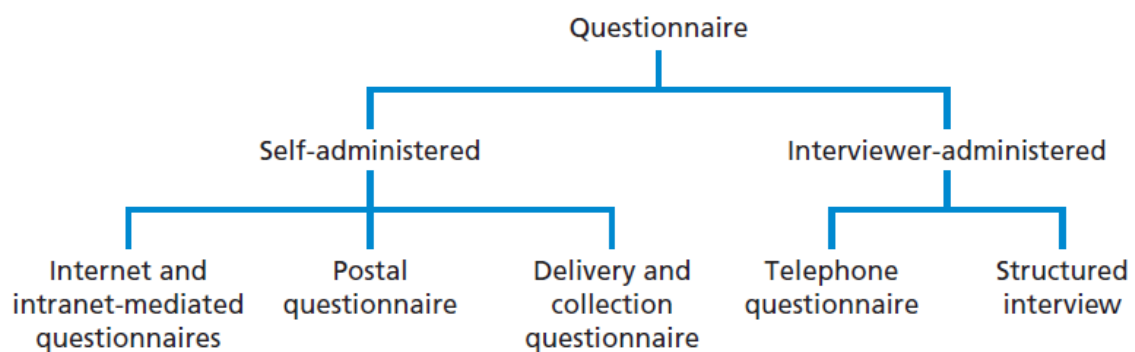


Figure 5.2: Types of Questionnaires (Saunders et al p.420., 2012)

Figure 5.2 depicts the various type of questionnaires. The type of questionnaire that was used for this research study was the self-administered questionnaire, which was completed by the respondents. The questionnaire was an internet-based questionnaire.

The survey tool used for the questionnaire was QuestionPro. The questions for the questionnaire were established to determine users' perceptions towards password policies. The questionnaire underwent a rigorous review process with the researcher and the supervisors until the final questions were chosen, for the questionnaire to be distributed. A pilot study was distributed to 5 respondents. The feedback from the pilot study included minor changes, such as changing the numbering of questions and modifying the logic related to branching questions. The positive reviews received from the pilot study indicated that respondents did not find the questions difficult to read or ambiguous. In addition, respondents found the questionnaire to be interesting and informative. After the pilot study, the feedback was immediately implemented by making the required changes. The changes were implemented and the researcher and supervisors did a final review before the questionnaire was distributed through Facebook and LinkedIn by means of a URL link. From within the questionnaire, respondents were required to open a further URL link to the 'Sample Password Policy' to answer Section 2 of the questionnaire.

The results of the survey were analysed with descriptive statistics. Descriptive statistics enable the researcher to describe and compare the data numerically (Saunders et al. p.502., 2012). This was done by providing simple summaries about the sample, for example frequency counts and distribution graphs, which can be found in Chapter 6, Section 6.5

5.6 Respondents and Ethical Consent

The respondents which the questionnaire targeted, were general computer users that use passwords on a regular basis. This included employees within small or large companies and students within academic institutions. The respondents were requested to indicate their demographic grouping based on gender, age and occupation. A total of 75 respondents completed the online questionnaire. The demographics of the respondents are discussed in detail in Chapter 6, Results and Findings, Section 6.2.

Before the respondents began the questionnaire, an ethical consent was presented to them stating that their participation in the survey was completely voluntary and confidential. The ethical consent from the questionnaire read as follows:

Your participation in this study is completely voluntary. Your survey responses will be strictly confidential and data from this research will be reported only in the aggregate. Your information will not be coded and will remain confidential.

5.7 Questionnaire Design

Questionnaires must be designed in such a way that the questions must be understood by the respondents and the respondents' answers must be understood by the researcher (Foddy, 1994). For the questionnaire to be valid, it must be reliable. Reliability ensures sure that the questionnaire is robust, providing consistent findings at different times and under different conditions (Saunders et al p.428., 2012). In this study, this was done by making sure that questions in the questionnaire were not ambiguous and open to misinterpretation by the respondents. With regard to the design of questions, most questions were developed from scratch by the researcher in order to determine users' perceptions towards the 'Sample Password Policy', as well as to identify users' coping strategies, while other questions were adapted from Choong, Theofanos, & Liu (2014). This specific study was chosen because the authors wanted to understand users' password management behaviours and perceptions with regard to password policies.

Most questionnaires consist of open-ended and closed questions. Open-ended questions allow respondents to provide their own answers, whereas closed questions allow respondents to select answers from a given list (Saunders et al p.432., 2012). The questionnaire related to this research study included both open-ended and closed questions. Furthermore, there are different types of closed questions. The types of closed questions chosen for this questionnaire included listing and rating questions. The listing questions offer a list of responses from which the respondents can choose. The responses consist of 'Yes/No', 'Applies/Does not apply', 'Don't know/Not sure' and 'Agree/Disagree' (Saunders et al p.433., 2012). Rating questions are often used to collect opinion data and typically use a Likert Scale rating where the respondents are asked how strongly they agree or disagree with a statement. Tables 5.4, 5.5 and 5.6 depict how the question types are linked to which questions.

The questionnaire relating to this research study was divided into three sections, namely: Demographics, Sample Password Policy and Behaviour and Coping Strategies. Refer to Appendix A1 for the complete questionnaire.

The Demographic section was divided into three parts, namely: gender, age and occupation. The gender group consisted of male and female options, the age group included ‘25 years and under’, ‘26 years to 35 years’, ‘36 years to 55 years’ and ‘56 years and over’. The occupation group included scholar, student, employee and pensioner. With regard to the occupation group, a comparison was done between the scholar/student group and employees to determine whether any significant differences existed between the groups. The results can be found in Chapter 6, Section 6.5.

The Sample Password Policy section aimed to determine users’ perceptions towards current password policies. The Sample Password Policy contained the common password policy elements, which were identified in Chapter 3, Section 3.3. The common password policy elements were integrated into the Sample Password Policy. The Password Generation section of the policy included the Password Length, Password Complexity and Password History elements. The Password Maintenance section of the policy included the Password Expiration and the general password recommendation section included the password recommendation element. This section of the questionnaire was also used to determine users’ perceptions with regard to the NIST password guidelines, by asking the respondents questions which related to the new NIST password policy guidelines (NIST SP 800-63B, 2016). Refer to Appendix A2 to view the Sample Password Policy.

The Behaviour and Coping Strategy section aimed to identify users’ coping strategies regarding password management. This section contained the coping strategies which were identified in Chapter 4, Section 4.3. By identifying users’ coping strategies, it can be determined which coping strategies are more common amongst users. The coping strategies identified in Chapter 4, Section 4.3, were used to ask the respondents which coping strategies they commonly adopt.

Table 5.1 depicts how the survey objectives are linked to the secondary objectives and the primary research objective.

SURVEY OBJECTIVE	OBJECTIVES
------------------	------------

<p>Survey objective 1 : To determine users' perceptions towards the Sample Password Policy</p> <p>Survey objective 3: To determine users' perceptions towards the new NIST SP 800-63B (2016).</p>	<p>Primary research objective: To determine users' perceptions regarding key elements of current password policy guidelines.</p>
<p>Survey objective 2: To determine coping strategies used by users regarding password management</p>	<p>Secondary objective 2: To determine human factors and coping strategies relating to password management</p>

Table 5.1: Survey Objectives Linked to Secondary Objectives

Table 5.1 depicts one survey objective linked to secondary objective 2 and two survey objectives linked to the primary research objective. The following subsections discuss the questions that were used to meet each of the survey objectives.

5.7.1 Survey Objective 1

Survey objective 1 aimed *to determine users' perceptions towards the Sample Password Policy*. The survey objective was achieved through questions depicted in Table 5.2. As mentioned previously, the question type of each question is also shown in Table 5.2.

Q#	QUESTION	TYPE
2.1	How do you feel about the prescribed password minimum length being 8 characters?	Rating question
2.2	How do you feel about the prescribed password maximum length being 16 characters?	Rating question
2.2a	Based on your answer from Question 2.2, why do you feel this way?	Open-ended
2.4	Do you feel that passwords should have composition requirements?	Rating question
2.7	To what extent do you agree or disagree that the general password recommendations are helpful?	Rating question
2.9	Would you find the sample password policy difficult to adhere to?	List question
2.9a	If answered "Yes", what section(s) makes the password policy difficult to adhere to?	List question
2.9b	Based on your answer from Question 2.9.a, why would you find the section(s) difficult to adhere to?	Open-ended

Table 5.2: Survey Objective 1 Questions

From the users' responses, it could be determined which aspects of the password policy users struggle with and how users feel towards the sample password policy. The users' perceptions towards the key elements of password policies were also determined from the sample password policy section. Some of the questions that formed part of this section do not feature here as they link to the NIST password

guidelines. These questions, 2.3, 2.3a, 2.4, 2.5, 2.6 and 2.8 are depicted in Table 5.4. Question 2.4 is displayed in both Table 5.2 and Table 5.4 as it also relates to the new NIST password guideline.

5.7.2 Survey Objective 2

Survey objective 2 aimed **to determine coping strategies used by users regarding password management**. This survey objective was achieved through the questions depicted in Table 5.3. As mentioned previously, some of the questions were adapted from a previous study conducted by Choong et al (2014). These questions included Questions 3.2 and 3.4.

Q#	QUESTION	TYPE
3.1	How often do you use the same password for different accounts?	List question
3.1a	If you answered Always, Often or Sometimes, why do you use the same password for different accounts?	Open-ended
3.2	What strategies do you use to create passwords?	List question
3.3	When constructing a password, which characters do you feel should be included? Please choose all that apply	List question
3.4	How do you keep track of your passwords?	List question
3.5	Which of the following coping strategies do you usually adopt?	List question
3.6	Which of the following Single Sign-On options do you use?	List question

Table 5.3: Survey Objective 2 Questions

The questions in Table 5.3 helped to identify which coping strategies are more common amongst the respondents with regard to password management. Questions 3.7 and 3.7a do not appear in Table 5.3 as they do not relate to survey objective 2 or any of the survey objectives, but instead aim to determine if respondents have attended any awareness or educational programmes relating to passwords.

5.7.3 Survey Objective 3

Survey objective 3 aimed **to determine users' perceptions towards the new NIST SP 800-63B (2016)**. This survey objective was achieved through the questions depicted in Table 5.4. Users were not made aware that these questions related to the new NIST standard. These questions were interspersed with other questions to ensure that they were not easily identified as being from the new NIST standard.

Q#	QUESTION	TYPE
2.3	How would you feel if passwords maximum prescribed length was increased to 64 characters?	Rating question
2.3a	Based on your answer from Question 2.3, why do you feel this way?	Open-ended
2.4	Do you feel that passwords should have composition requirements?	Rating question
2.5	Would you like the option of using spaces and emoji's (smiley face ☺,sad face ☹) in your passwords?	List question
2.6	How often would you prefer to change your passwords?	List question
2.8	Would you like the option to have your newly created passwords automatically checked by the system against a list of commonly compromised passwords before committing to it?	List question
2.8a	Based on your answer from Question 2.8, why do you feel this way?	Open-ended

Table 5.4: Survey Objective 3 Questions

The questions depicted in Table 5.4 would help identify users' perceptions towards these new guidelines and could help determine whether these perceptions should be considered when deciding to adapt existing password policies or develop new password policies.

5.8 Conclusion

This chapter discussed the research process that was followed for this research study. The inductive approach was used and the research study used various research methods, such as literature reviews, content analysis, argumentation and a survey in the form of a questionnaire. The convenience sampling technique was used for this research study to target respondents for the questionnaire. The design of the questionnaire was presented, as well as the types of questions used such as open-ended and closed questions. The following chapter presents the results and findings of the data collected from the questionnaire.

Chapter 6 : Results and Findings

The aim of this chapter is to report the general results and findings from the questionnaire. These results will help identify users' perceptions towards password policies as well as identify users' coping strategies.

6.1 Introduction

The researcher conducted an online survey in the form of a questionnaire to determine human factors and coping strategies relating to password policies, as well as to determine users' perceptions regarding password management and password recommendations. The questionnaire was divided into three sections namely: Demographics, Sample Password Policy and Behaviour and Coping Strategies. The design of the questionnaire and process are explained in detail in Chapter 5, Section 5.7.

This chapter is structured as follows: Section 6.2 presents the demographics of the research study, followed by the Sample Password Policy results and findings in Section 6.3. Section 6.4 discusses the behaviour and coping strategy results and findings, while Section 6.5 compares and addresses the student/scholar and employees' results and findings. Section 6.6 concludes this chapter.

6.2 Research Study Demographics

This section summarises the demographics of the survey, as depicted in Table 6.1. A total of 75 respondents participated in the study.

DEMOGRAPHICS		
Gender of respondents	Number of responses	Percentage
Male	42	56.0%
Female	33	44.0%
Age Group	Number of responses	Percentage
25 years and under	32	42.7%
26 years to 35 years	18	24.0%
36 years to 55 years	23	30.7%
56 years and above	2	2.6%
Occupation	Number of responses	Percentage
Scholar	4	5.3%
Student	25	33.3%
Employee	46	61.3%
Pensioner	0	0.0%

Table 6.1: Research Study Demographic Results (n=75)

As depicted in Table 6.1, the majority of respondents were male with 56% and 44% of respondents were female. The age group of respondents which had the biggest total was the 25 years and under group with 42.7% and the 36 to 55 years group with 30.7%. With regard to the occupation of respondents, the majority of respondents were employees with 61.3%, followed by students with 33.3%.

The next section discusses the results and findings from the Sample Password Policy section of the questionnaire. The Sample Password Policy is provided in Appendix A2.

6.3 Sample Password Policy Results and Findings

As stated earlier, the number of respondents for the survey was 75. However, in this section, there were three questions which only recorded the responses of 74 respondents, namely Question 2.4, Question 2.5 and Question 2.6. Table 6.2 depicts the responses to Question 2.1, which addressed the respondents' attitudes towards the prescribed password minimum length being 8 characters.

2.1 How do you feel about the prescribed password minimum length being 8 characters?		
Likert Scale options	Number Responses	Percentage Responses
Very satisfied	25	33.3%
Slightly satisfied	16	21.3%
Neutral	24	32.0%
Slightly dissatisfied	9	12.0%
Very dissatisfied	1	1.3%

Table 6.2: Password Minimum Length of 8 (n=75)

Table 6.2 depicts that 54.6% of respondents felt relatively satisfied about the prescribed password minimum length being 8 characters. The 54.6% combined the percentages of 'Very satisfied' and 'Slightly satisfied'. 32% of respondents felt neutral about the password minimum length being 8 characters, and the remaining 13.3% of the respondents were dissatisfied with the minimum password length requirement.

2.2 How do you feel about the prescribed password maximum length being 16 characters?		
Likert Scale options	Number Responses	Percentage Responses
Very satisfied	18	24.0%
Slightly satisfied	7	9.3%
Neutral	19	25.3%
Slightly dissatisfied	18	24.0%
Very dissatisfied	13	17.3%

Table 6.3: Password Maximum Length of 16 (n=75)

With regard to Question 2.2, Table 6.3 depicts that 33.3% of the respondents felt satisfied with the maximum password length being 16 characters, whereas 41.3% of respondents felt dissatisfied about this. This question was followed by an open-ended question to determine how users actually felt towards the maximum prescribed password length of 16 characters. Through the open-ended question, respondents made the following comments regarding a maximum prescribed password length of 16 characters:

- Makes the password '*too long*',
- Makes the password '*harder to remember the passwords and easier to make mistakes while typing*'.
- Makes the passwords '*harder to crack*',
- Respondents further commented that '*Passwords should not have a limit or should be longer than 16 characters.*'

It can be determined that, although the respondents mentioned that passwords of 16 characters were too long, they also knew that it would be more secure and harder for attackers to crack.

2.3 How would you feel if passwords maximum prescribed length was increased to 64 characters?		
Likert Scale Options	Number Responses	Percentage Responses
Very Satisfied	11	14.7%
Slightly satisfied	4	5.3%
Neutral	15	20.0%
Slightly dissatisfied	5	6.7%
Very dissatisfied	40	53.3%

Table 6.4: Increased Password Maximum Length of 64 (n=75)

Table 6.4 indicates that 60% of respondents would be relatively dissatisfied if the maximum password length was increased to 64 characters and 19.9% of respondents felt relatively satisfied about this. This question was followed by an open-ended question to determine how users actually felt towards the maximum prescribed password length being increased to 64 characters. From the open-ended question, some users stated the following regarding a maximum prescribed password length of 64 characters:

- Passwords would be '*more secure*',

- *'It is too long and I would not be able to remember my password'*,
- *'64 characters is too much and would only be sufficient for people with long passwords'*,
- *'My passwords are not even longer than 16 characters'*.

As can be seen from the comments, Question 2.3 seems to have been misinterpreted by some respondents. The question did not indicate that passwords **should** be 64 characters in length, but rather, that the maximum length of passwords **could** be increased to 64 characters.

2.4 Do you feel that passwords should have composition requirements?		
Likert Scale options	Number Responses	Percentage Responses
Strongly agree	28	37.8%
Agree	24	32.4%
Undecided/Neutral	18	24.3%
Disagree	4	5.4%
Strongly disagree	0	0.0%

Table 6.5: Password Composition Requirements (n=74)

With regard to Table 6.5, Question 2.4 which asked how the respondents felt about composition requirements, 70.2% of respondents agreed to a certain extent that passwords should have composition requirements. 24.3% of respondents were undecided/neutral, while a small percentage of 5.4% of the respondents disagreed that passwords should contain composition requirements. The results of Question 2.4, therefore, revealed that the majority of respondents agreed that passwords should have composition requirements.

2.5 Would you like the option of using spaces and emoji's in your passwords?		
Options	Number Responses	Percentage Responses
Yes	31	41.9%
No	31	41.9%
Undecided	12	16.2%

Table 6.6: Emojis and Spaces in Passwords (n=74)

With regard to Table 6.6, Question 2.5, which asked the respondents whether they would like the option of using spaces and emoji's in their passwords, the results were split equally with 41.9% stating 'Yes' and 41.9% stating 'No'. The results indicate that some of the users would like the option of using emoji's and spaces in their passwords, whereas others do not wish to use emoji's and spaces in their passwords.

2.6 How often would you prefer to change your passwords?		
Options	Number Responses	Percentage Responses
Every 60 days	15	20.3%
Every 90 days	13	17.6%
Every 120 days	14	18.9%
Never	32	43.2%

Table 6.7: Password Change (n=74)

Table 6.7, Question 2.6 indicates that 43.2% of respondents do not wish to change their passwords ever, whereas 20.3% of respondent's stated that they would prefer to change their passwords 'Every 60 days'. 17.6% of respondents preferred to change their passwords 'Every 90 days' and 18.9% of respondents preferred 'Every 120 days'.

2.7 To what extent do you agree or disagree that the general password recommendations are helpful?		
Likert Scale Options	Number Responses	Percentage Responses
Strongly agree	19	25.3%
Agree	41	54.7%
Undecided/Neutral	12	16.0%
Disagree	3	4.0%
Strongly disagree	0	0.0%

Table 6.8: General Password Recommendations (n=75)

Table 6.8, Question 2.8 indicates that a total of 80.0% of respondents agreed to some extent that the general password recommendations of the Sample Password Policy were helpful. This 80.0% combined the 54.6% of 'Agree' and 25.3% of 'Strongly agree'. Therefore, a large percentage of respondents agreed that the general password recommendations were helpful.

2.8 Would you like the option to have your newly created passwords automatically checked by the system against a list of commonly compromised passwords before committing to it?		
Options	Number Responses	Percentage Responses
Yes	57	76.0%
No	11	14.7%
Undecided	7	9.3%

Table 6.9: Password checking (n=75)

With regard to Table 6.9, Question 2.8, 76.0% of respondents indicated 'Yes' they would like to have their passwords checked against commonly compromised passwords, which shows that the majority of respondents would like this option. This question was followed by an open-ended question to determine how users actually

felt about this option. With regard to the open-ended question, respondents stated that this option:

- Could *'reduce the risk of passwords being compromised'*,
- Would allow them to *'feel reassurance that their password is strong and safe'*.
- Would allow them to *'like the option of seeing how secure my password is which will also help in create stronger passwords'*.

However, a few respondents were concerned that the system would store their passwords after checking them and thought that the systems could easily be compromised. For example, respondents said that they *'don't want it to be known to anybody not even a system'* and *'then the system will store my password and have access to it'* and *'the system could be compromised and someone could have access to your passwords'*.

2.9 Would you find the Sample Password Policy difficult to adhere to?		
Options	Number Responses	Percentage Responses
Yes	11	14.7%
No	51	68.0%
Undecided	13	17.3%

Table 6.10: Password Policy (n=75)

With regard to Table 6.10, Question 2.9 indicates that 68% of respondents indicated 'No', the Sample Password Policy would not be difficult to adhere to, whereas 14.7% of respondents indicated 'Yes'. This question was also expanded to determine which sections make the password policy difficult to adhere to. From Question 2.9a, 50% of respondents indicated that the Password Maintenance Section was the most difficult to adhere to. This question was followed by an open-ended question to determine what makes the various sections difficult to adhere to. Respondents stated that:

- *'they have multiple passwords and they have to create a new one every few months and do not like the idea of changing their passwords'*,
- *'they do not like the special characters in the passwords'*,
- *'to not write their passwords down on paper to help them remember would be a problem'*.

The overall results and findings of Section 2, Sample Password Policy, indicate that the respondents did not find the Sample Password Policy difficult to adhere to. However, it was discovered that users struggled with certain guidelines in the Sample Password Policy. With regard to the Password Generation Section, respondents found the prescribed password maximum length of 16 characters to be too long and difficult to remember. Some respondents also misinterpreted the prescribed password maximum length, as some respondents stated that their passwords do not even reach 16 characters. The Password Maintenance Section results indicated that the respondents do not wish to ever change their passwords. The Password Recommendations Section indicates that the respondents found the proposed guidelines to be helpful in better protecting their passwords. These guidelines included:

- *‘Not to share your passwords with anyone: family, friends, colleagues, strangers, superiors’,*
- *‘Do not use the “Remember Password” feature of applications’,*
- *‘Do not store passwords in a file on any computer system unencrypted’,*
- *‘Ensure you do not allow someone to see you type in your password (shoulder surfing)’*

The following section discusses Section 3, Behaviour and Coping Strategies results and findings.

6.4 Behaviour and Coping Strategies Results and Findings

The section’s design and process are explained in more detail in Chapter 5, Section 5.7. Table 6.11 depicts how often the respondents use the same password for different accounts.

3.1 How often do you use the same password for different accounts?		
Likert Scale Options	Number Responses	Percentage Responses
Always	19	25.3%
Often	36	48.0%
Sometimes	15	20.0%
Seldom	5	6.7%
Never	0	0%

Table 6.11: Password Reuse (n=75)

Table 6.11 shows that 73.3% of respondents answered 'Always' or 'Often' and thus frequently use the same password for different accounts. It was interesting to note that 0% of the respondents 'Never' use the same password across different accounts. This question was expanded on in Question 3.1a, as shown in Table 6.12, to understand why users use the same password for different accounts. The responses of 70 respondents are shown in Table 6.12, as they were the respondents who answered 'Always', 'Often' or 'Sometimes'.

3.1a If you answered Always, Often or Sometimes, why do you use the same password for different accounts?		
Options	Number Responses	Percentage Responses
Find it difficult to come up with a new password	16	22.9%
Do not want to remember multiple passwords	44	62.9%
Find it difficult to remember multiple passwords	36	51.4%
Easier to remember	38	54.3%
Other	2	2.8%

Table 6.12: Password Reuse Reason (n=70)

With regard to Question 3.1a, respondents could choose multiple answers. From Table 6.12 it can be seen that 62.9% of respondents use the same password for different accounts as they do not want to remember multiple passwords, whereas 51.4% of respondents stated that they find it difficult to remember multiple passwords. From Table 6.12 it can be determined that users do not want to remember multiple passwords and that they reuse passwords across multiple accounts because it is easier to remember the password.

3.2 What strategies do you use to create passwords?		
Options	Number Responses	Percentage Responses
Make minor change(s) to an existing password (e.g. %stevie1,#stevie2)	49	65.3%
Use a common name, word or phrase(e.g. how you doing12?)	20	26.7%
Use meaningful mnemonic (e.g 2beOrnOt@toBee from "to be or not to be")	19	25.3%
Use random combination of words , letters or characters	22	29.3%
Use character repetitions (e.g !!!!AAAbbbb9999)	4	5.3%
Use existing passwords from other accounts	35	46.7%
Use password managers (e.g Lastpass, Roboform)	2	2.7%
Use Single Sign-on (e.g. Facebook login, Google login)	19	25.3%

Table 6.13: Password Generation Strategies (n=75)

With regard to the results of Question 3.2, certain results are highlighted. For this question, the respondents were allowed to select multiple answers that applied to their password generation strategies. This question asked the respondents what strategies they use to create their passwords. As can be seen from Table 6.13, 65.3% of respondents ‘*Make minor changes to an existing password*’, whereas 46.7% of respondents ‘*Use existing passwords from other accounts*’ to create their passwords. However, there is a mismatch with this response as seen from Question 3.1, which asked how often they reuse the same password across different accounts. There was a larger percentage of respondents that reused passwords across accounts. Further, 29.3% of the respondents use random combinations of words, letters and numbers to create their passwords and 26.7% of respondents use a common name, word or phrase to create their passwords. 25.3% of respondents reported the use of Single Sign-On, while 25.3% of respondents reportedly use meaningful mnemonics in order to create their passwords.

3.3 When constructing a password, which characters do you feel should be included?		
Options	Number Responses	Percentage Responses
Lowercase	55	73.3%
Uppercase	62	82.7%
Numbers	64	85.3%
Special characters	52	69.3%
Emoji’s	14	18.7%
Spaces	10	13.3%

Table 6.14: Password Composition Requirements (n=75)

In Question 3.3, the respondents could select multiple answers. The results that are presented in Table 6.14 depict that 85.3% of respondents are of the opinion that numbers should be included in passwords. 82.7% of respondents are of the opinion that uppercase characters should be included in passwords and 73.3% believe that lowercase characters should be included. It can be seen that the special characters results (69.3%) from Table 6.14 link back to Table 6.5 where respondents stated that passwords should contain special characters. With regard to emoji’s and spaces, both received relatively low percentages with 18.7 % for emoji’s and 13.3% for spaces.

3.4 How do you keep track of your passwords?		
Options	Number Responses	Percentage Responses
Memorise the password	61	81.3%
Use Single sign-on	26	34.7%
Use "forget password" feature	29	38.6%
Let browser autofill	17	22.6%
Rely on hints provided by systems	10	13.3%
Save in a document/file protected with encryption	10	13.3%
Save in a document/file not protected	2	2.7%
Share with friend or colleague	0	0%
Store in encrypted electronic devices	6	8.0%
Use mnemonics	8	10.7%
Use password management software	5	6.7%
Write down on paper but disguise in some way	16	21.3%
Write entire password down on paper and store securely in a locked location	7	9.3%
Write entire password down on paper and place in a non-locked location	2	2.7%

Table 6.15: Password Tracking (n=75)

In Question 3.4, respondents could select multiple answers that were applicable to them. As seen from Table 6.15, the results indicate that 81.3% of respondents memorise their password to keep track of them. The second highest tracking behaviour respondents use, with 38.6%, was the 'Use forgot password feature' and 34.7% of respondents reported using 'Single Sign-On' to keep track of their passwords. 0% of respondents indicated that they do not share their passwords with friends or colleagues, which is very positive as this is a best practice. From Table 6.15, it can be seen that the recommended password practices, such as memorising passwords and using Single Sign-On, are being utilised more by the respondents than poor password practices, such as the 'forgot password feature', sharing of passwords and writing down of passwords.

3.5 Which of the following coping strategies do you usually adopt?		
Options	Number Responses	Percentage Responses
Reuse my password for multiple accounts	65	86.7%
Share my passwords with others	1	1.3%
Write down my password on paper	15	20.0%
Write down my password in a document (electronic)	8	10.7%
Use a password manager	6	8.0%
Use Single Sign-On	21	28.0%
Create weak password	5	6.7%
Do not change my password unless forced to change it	46	61.3
Other	2	2.7%

Table 6.16: Password Coping Strategies (n=75)

With regard to the results of Question 3.5, certain results are highlighted. In this question, the respondents could select multiple answers that applied to them. The results in Table 6.16 indicate that 86.7% of respondents 'Reuse passwords for multiple accounts' and 28.0% of respondents 'Use Single Sign-On' as coping strategies. 61.3% of respondents 'Do not change their passwords unless forced to change it'. The writing of passwords had a combined percentage of 30.7%, made up by combining the results for 'Write down my password on paper' with 'Write down my password in a document (electronic)'. The most common coping strategy is the password re-use, which is in line with other research studies, such as Inglesant & Sasse (2010); Stobert & Biddle (2015) and Wash, Rader, Berman, & Wellmer (2016).

3.6 Which of the following Single Sign-On options do you use?		
Options	Number Responses	Percentage Responses
Facebook Login	53	70.7%
Twitter Login	7	9.3%
Google Login	43	57.3%
Microsoft Login	13	17.3%
Apple Login	10	13.3%
Linkedin Login	14	18.7%
None	13	17.3%
Other	3	4.0%

Table 6.17: Single Sign-On (n=75)

For Question 3.6 the respondents could select multiple answers that apply to them. The results from Table 6.17 indicate that Facebook login is the most popular Single Sign-On with 70.7%, followed by Google login with 57.3%. However, 17.3% of respondents indicated that they do not use any Single Sign-On. This question may have been misinterpreted as the previous question, Question 3.5 revealed that 21 respondents used Single Sign-On as a coping strategy, while Question 3.6 seems to have more respondents that used Single Sign-On. It may be due to the fact that the respondents might not know what Single Sign-On is.

3.7 Have you been part of any awareness or educational programs with regard to passwords?		
Options	Number Responses	Percentage Responses
Yes	20	26.7%
No	55	73.3%

Table 6.18: Awareness or Education on Passwords (n=75)

The results of Table 6.18 indicate that 73.3% of respondents have not been part of any awareness or educational programmes on passwords, whereas 26.7% of

respondents have. The number of respondents that have not been part of any awareness or educational programme is a concern, as users might not know what constitutes a secure password and might not know how to better protect their passwords. This could result in users adopting insecure coping strategies. Question 3.7a determined where the respondents have attended password awareness or educational programmes.

3.7a Where have you attended the education or received awareness programs on passwords?		
Options	Number Responses	Percentage Responses
School	3	15.0%
University	17	85.0%
Work	8	40.0%
On my own(website, YouTube, videos)	4	20.0%
Other	0	0.0%

Table 6.19: Awareness and Education Programmes Attended (n=20)

Question 3.7a allowed the respondents who answered ‘Yes’ to attending awareness or educational programmes, to select multiple answers that applied to them. The results from Table 6.19 indicate that 85.0% of respondents have been part of password awareness or educational programmes at ‘University’, while 40.0% of respondents have received it at ‘Work’.

The results and findings of Section 3 Behaviour and Coping Strategies, of the questionnaire, indicate that the respondents often reuse their passwords across many accounts. This is due to the fact that respondents do not want to, or cannot, remember multiple passwords. With regard to what strategies the respondents use to create passwords, it was found that they make minor changes to existing passwords or use existing passwords from other accounts. In order for them to keep track of their passwords, it was found that the respondents rely on memorisation, use the ‘forgot password’ feature and use Single Sign-On. Further, it was found that the majority of respondents have not been part of any awareness or educational programmes with regard to passwords. This may indicate a problem and could play a role in users’ password management behaviours.

The next section compares the employees and student/scholar results to determine whether any differences exist between these groups

6.5 Comparison of Employee and Student/Scholar Group

This section compares the results of the employee and student/scholar groups to determine whether there was any major difference between the two groups. The students and scholars were combined and represented as one group. The student/scholar group consisted of 29 respondents and the employee group consisted of 46 respondents.

With regard to the results of Section 2, Sample Password Policy, there were a number of differences between the student/scholar and employee groups. The results of Questions 2.4 and 2.8 showed no major differences between the student/scholar and employee groups. The results from these questions only had between 0 and 10% difference and, therefore, did not indicate any noteworthy difference. When asked which parts of the Sample Password Policy they found most difficult to adhere to, both groups stated that the Password Maintenance section was the most difficult section to adhere to. However, there were some questions in Section 2 Sample Password Policy, where there were some differences between the two groups. The results from these questions are highlighted, as there was a 10% or greater difference between the two groups. Figures 6.1, 6.2, 6.3, 6.4, 6.5, 6.6 and 6.7, illustrate the differences between the two groups for questions 2.1, 2.2, 2.3, 2.5, 2.6, 2.7 and 2.9 respectively.

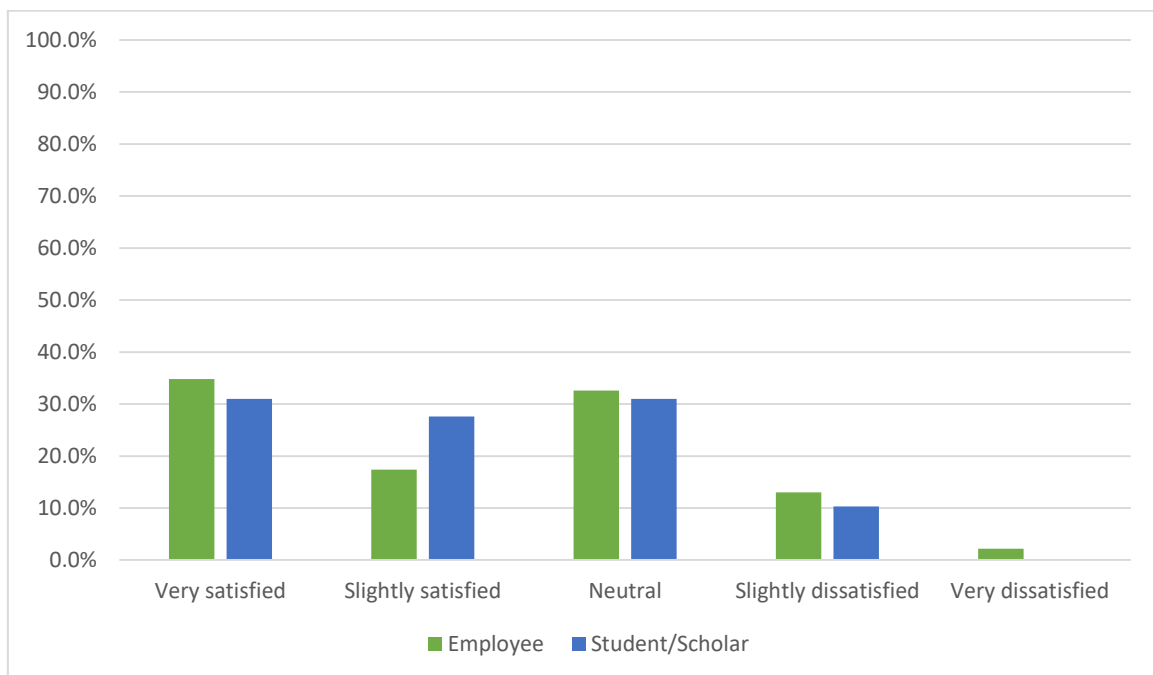


Figure 6.1: Question 2.1 Results

Question 2.1 asked the respondents how they felt about the prescribed password minimum length being 8 characters. From Figure 6.1, it can be determined that the noteworthy difference between the two groups is with the “Slightly satisfied” Likert scale option, were 17.4% of employees and 27.6% of students/scholars were slightly satisfied about the prescribed minimum password length being 8 characters in length.

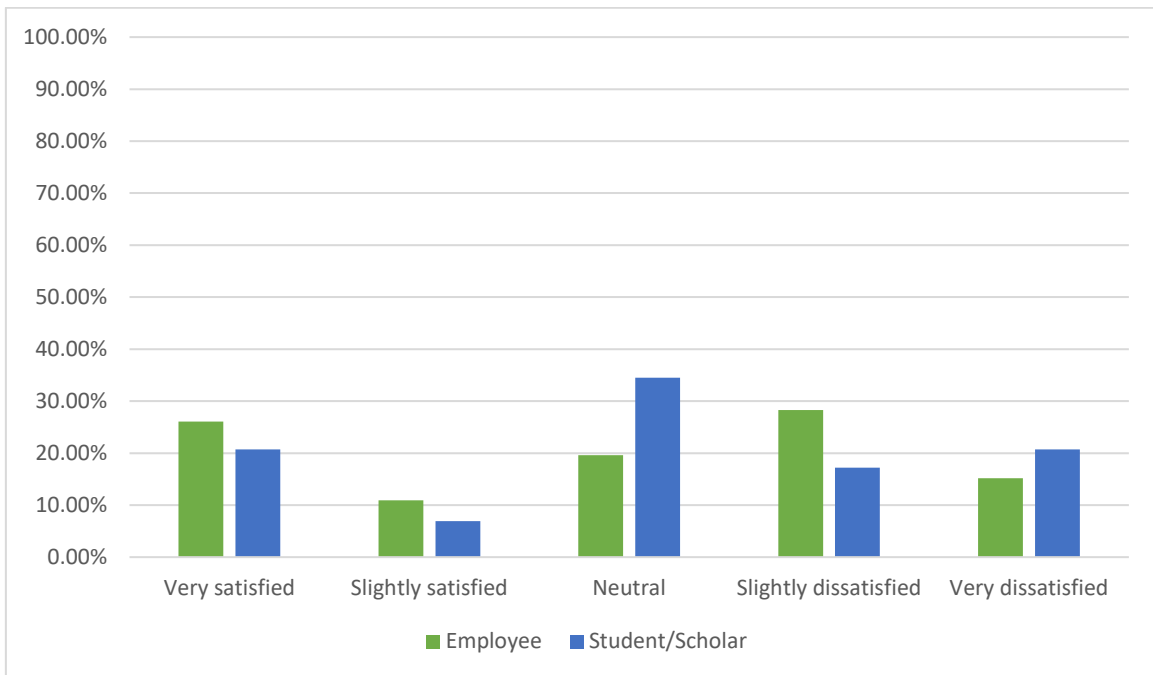


Figure 6.2: Question 2.2 Results

Question 2.2 asked the respondents how they felt about the prescribed maximum password length being 16 characters long. From Figure 6.2 it can be determined that the employee group was more dissatisfied about the maximum length being 16 characters while the student/scholar group felt neutral.

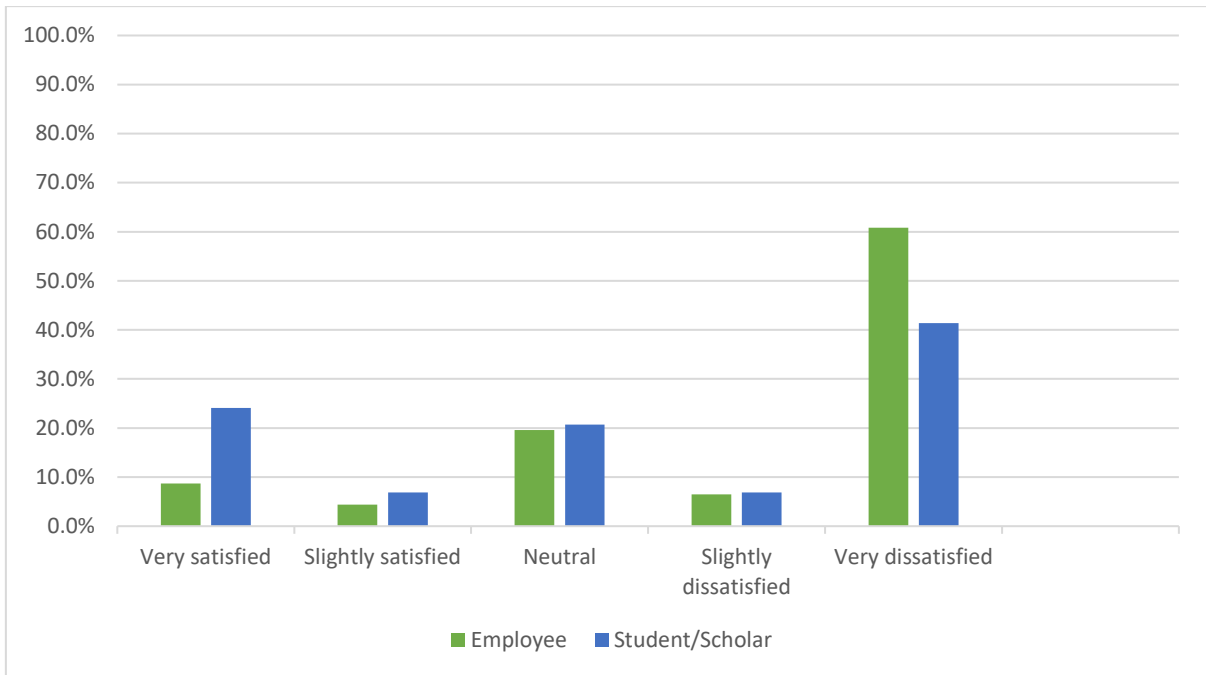


Figure 6.3: Question 2.3 Results

Question 2.3 asked the respondents how they would feel if the prescribed maximum password length was increased to 64 characters. From Figure 6.3 it can be identified that the largest differences between the two groups relate to the ‘Very satisfied’ and ‘Very dissatisfied’ Likert scale options. The student/scholar group would feel more satisfied if the maximum prescribed password was increased to 64 characters, while the employees were more dissatisfied than the student/scholar group about the maximum prescribed password length.

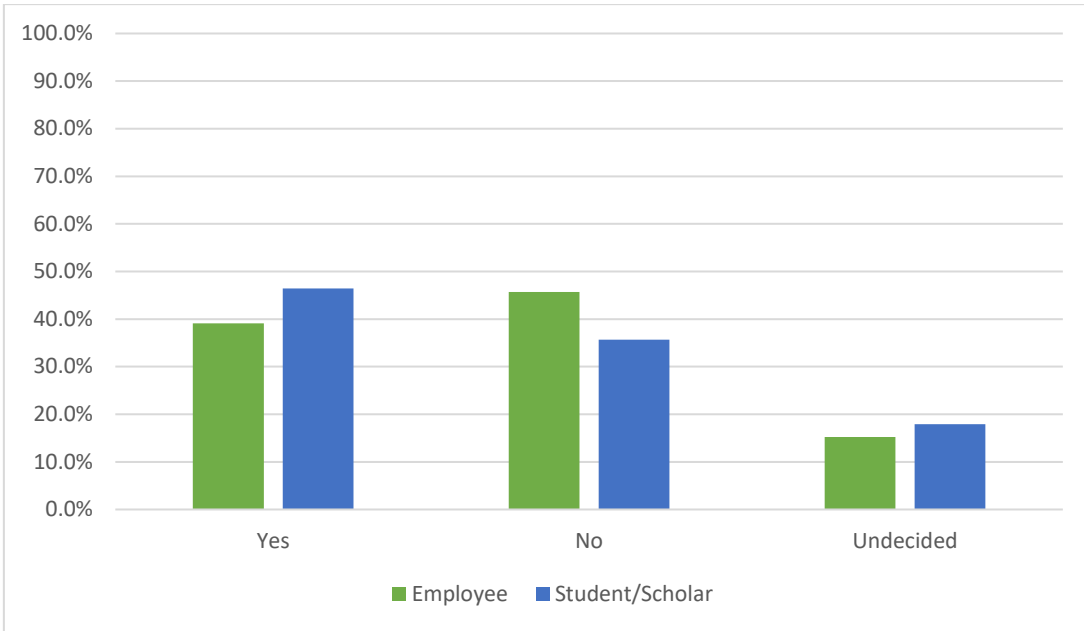


Figure 6.4: Question 2.5 Results

Question 2.5 asked the respondents if they would like the option of using spaces and emoji's in their passwords. From Figure 6.4 it can be determined that 45.7% of employees stated 'No' to this option compared to the 35.7% of the student/scholar group. 46.4% of students/scholars stated 'Yes' to this option. The student/scholar group preferred the option of using these characters in their passwords.

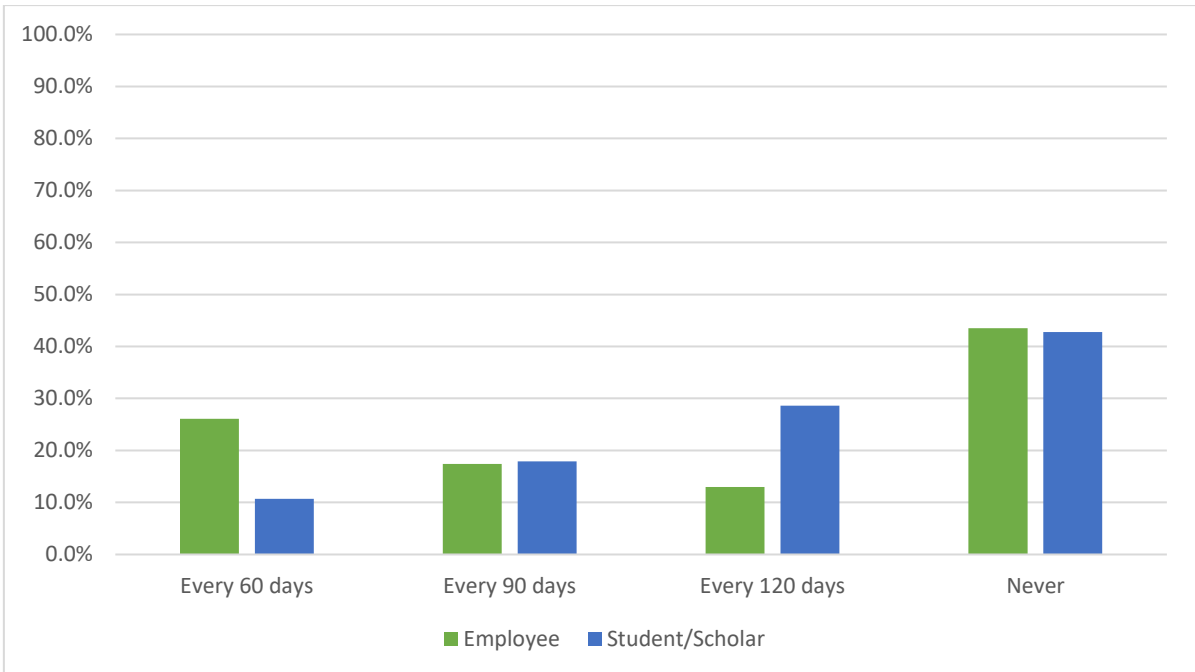


Figure 6.5: Question 2.6 Results

Question 2.6 asked the respondents how often they prefer to change their passwords. From Figure 6.5, it can be identified that employee and student/scholar groups prefer to 'Never' have to change their passwords, as the percentage difference between the groups was marginal. However, 26.1% of employees prefer to change their passwords 'Every 60 days' compared to 10.7% of the student/scholar group.

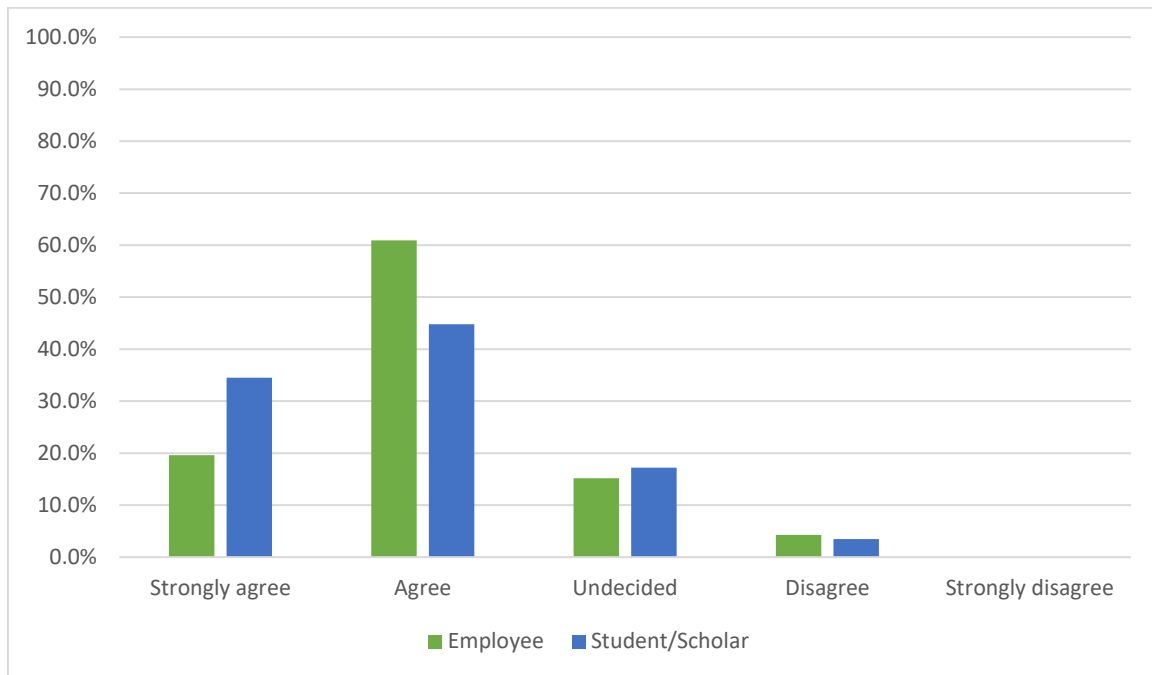


Figure 6.6: Question 2.7 Results

Question 2.7 asked the respondents if they felt that the general password recommendations were helpful or not. From Figure 6.6 it can be identified that both groups agree that the general password recommendations are helpful. There was only a slight difference in percentages between the employee group with 80.5% and the student/scholar group with 79.3%. The general password recommendations provided the employees and student/scholar groups with better ways to protect their passwords.

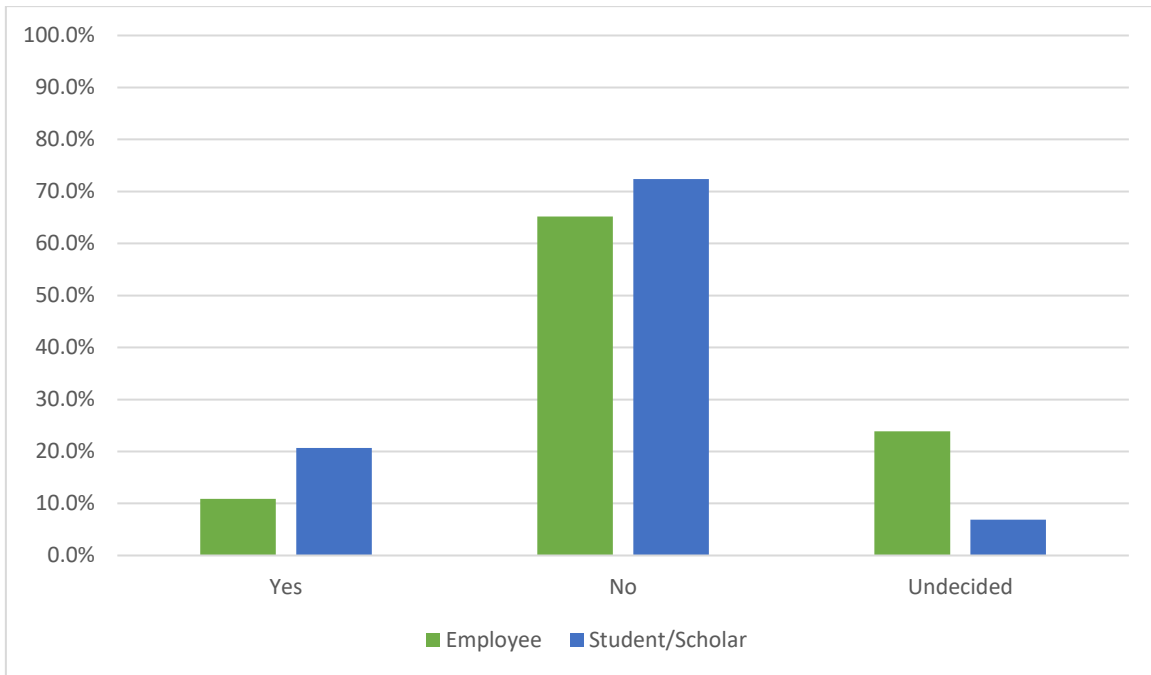


Figure 6.7: Question 2.9 Results

Question 2.9 asked the respondents if they found the Sample Password Policy difficult to adhere to. From Figure 6.7 it can be determined that the significant difference between the two groups was the '*Undecided*' option, with 23.9% of the employees and 6.9% of the student/scholar group being undecided. However, the employee group found the Sample Password Policy not difficult to adhere to.

With regard to Section 3 Behaviour and Coping Strategies, results from the questionnaire indicate that there were slight differences between the employee and student/scholar groups. The results of Question 3.1 showed that there was no noteworthy difference between the two groups. Figures 6.8, 6.9, 6.10, 6.11, 6.12, 6.13, 6.14 and 6.15 present the differences between the two groups with regard to Questions 3.1a, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7 and 3.7a respectively.

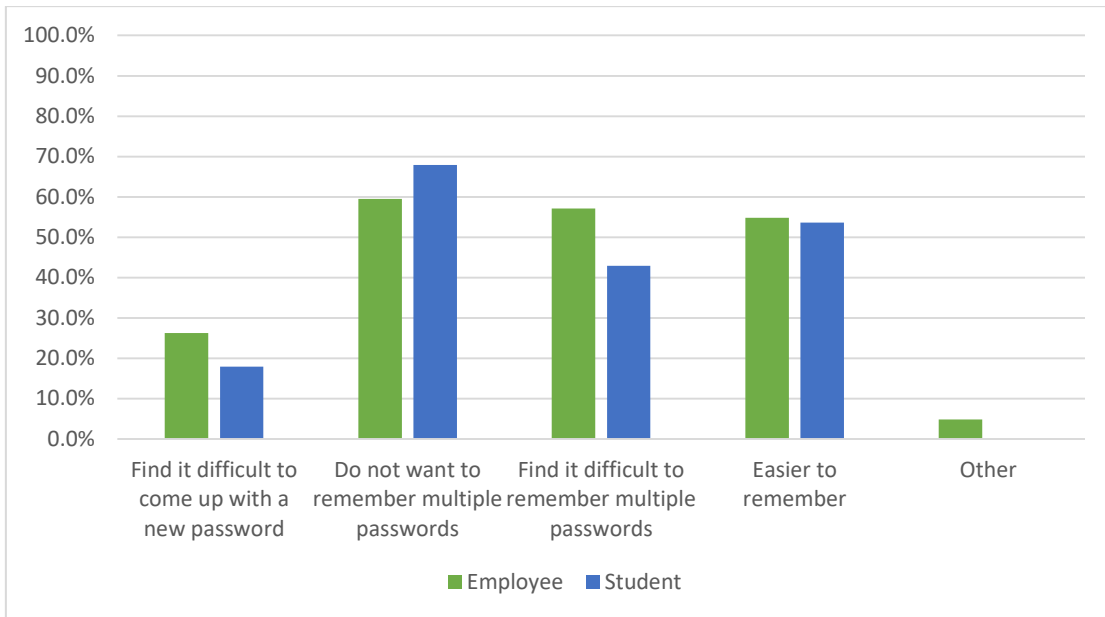


Figure 6.8: Question 3.1a Results

Question 3.1a, asked the respondents why they use the same password for different accounts. From Figure 6.8 it was determined that the noteworthy difference was for the 'Find it difficult to remember multiple passwords' option, with 57.1% of the employee group and 42.9% of the student/scholar group finding it difficult to remember multiple passwords.

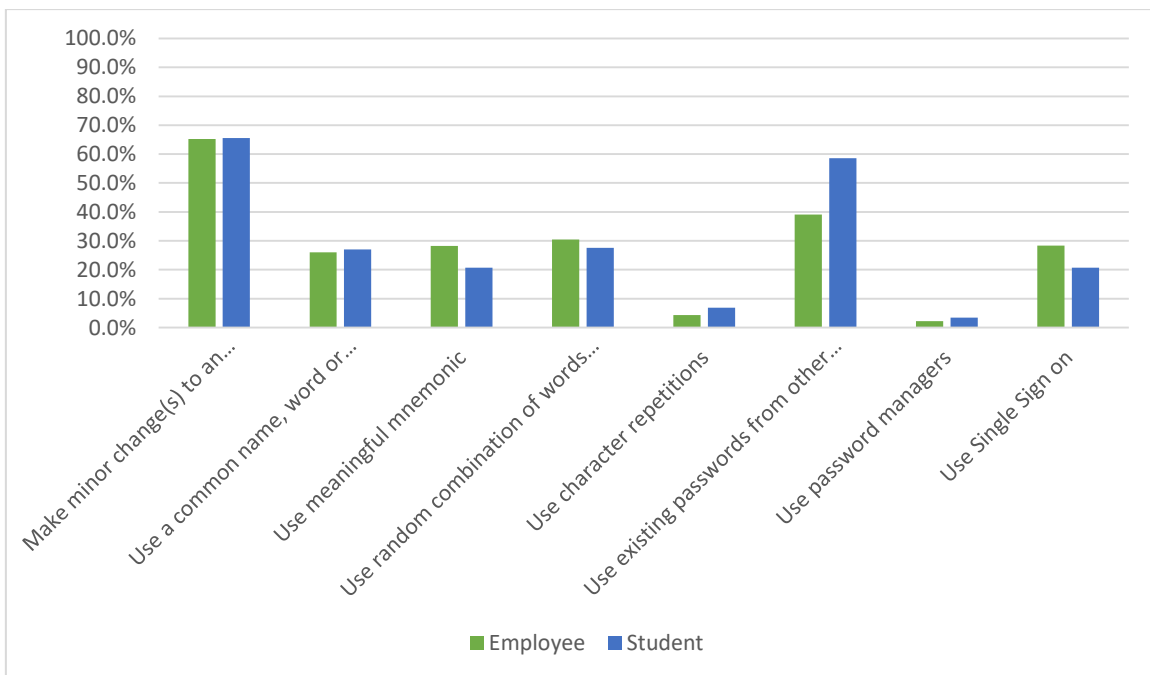


Figure 6.9: Question 3.2 Results

Question 3.2 asked the respondents what strategies they use to create passwords. From Figure 6.9 it can be determined that the employee and student/scholar groups had similar strategies for creating passwords. However, there was a noteworthy difference between the employee and student/scholar groups that ‘use existing passwords from other accounts’ to create passwords, where the student/scholar group used this strategy more often than the employee group.

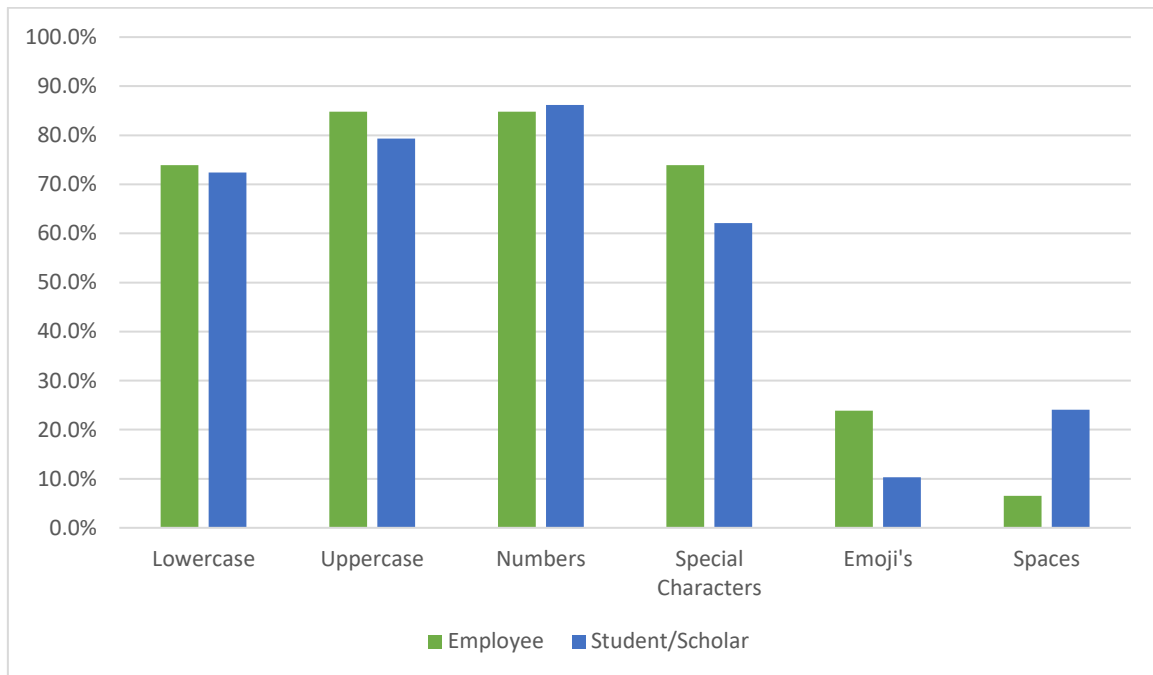


Figure 6.10: Question 3.3 Results

Question 3.3 asked the respondents, when constructing a password, which characters should be included in a password. From Figure 6.10 it can be determined that both groups were in agreement that passwords should contain lowercase and uppercase characters, numbers and special characters. However, with regard to having emoji's and spaces in the passwords, the two groups had some significant differences. With regard to the emoji's, 23.9% of the employee group were of the opinion that passwords should contain emoji's compared to the 10.3% of the student/scholar group. 24.1% of the student/scholar group were of the opinion that spaces should be included in passwords compared to 6.5% of the employee group..

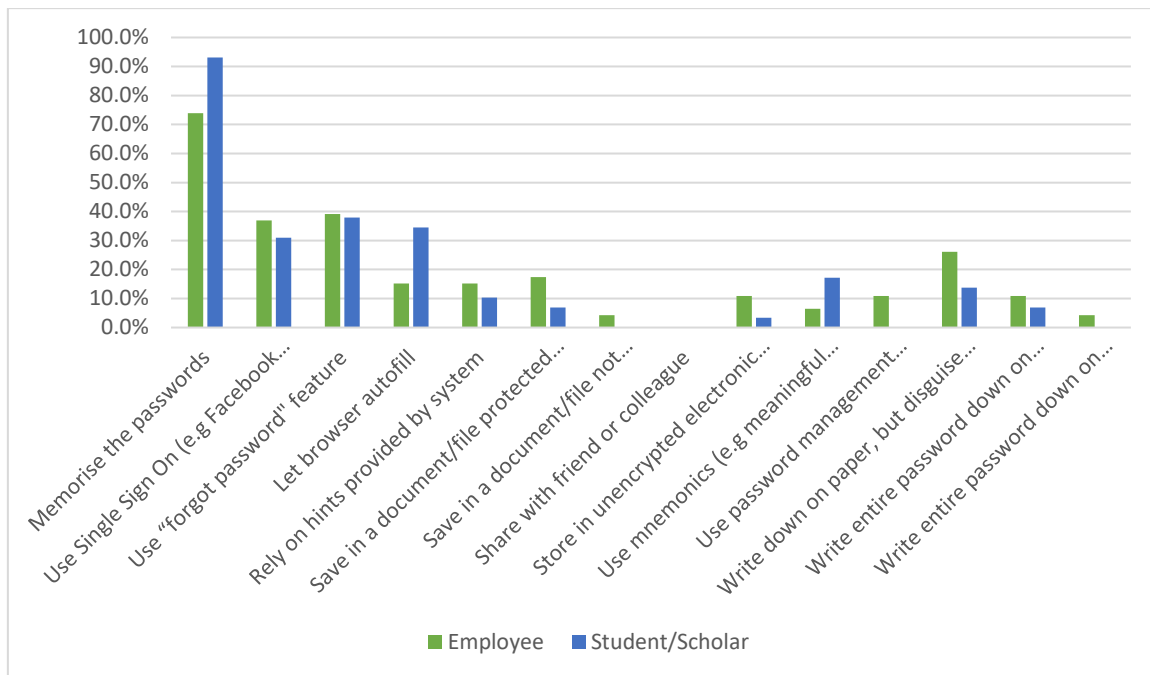


Figure 6.11: Question 3.4 Results

Question 3.4 asked the respondents how they keep track of their passwords. From Figure 6.11 it can be determined that the two groups had similar methods of keeping track of their passwords. However, there were some noteworthy differences, such as 93.1% of students/scholars relied more on memorisation compared to 73.9% of employees. 34.5 % of the student/scholar group 'let the browser autofill' their passwords compared to 15.2% of employees. 26.1 % of employees 'write down their passwords on paper but disguise it in some way' compared to 13.8% of the student/scholar group.

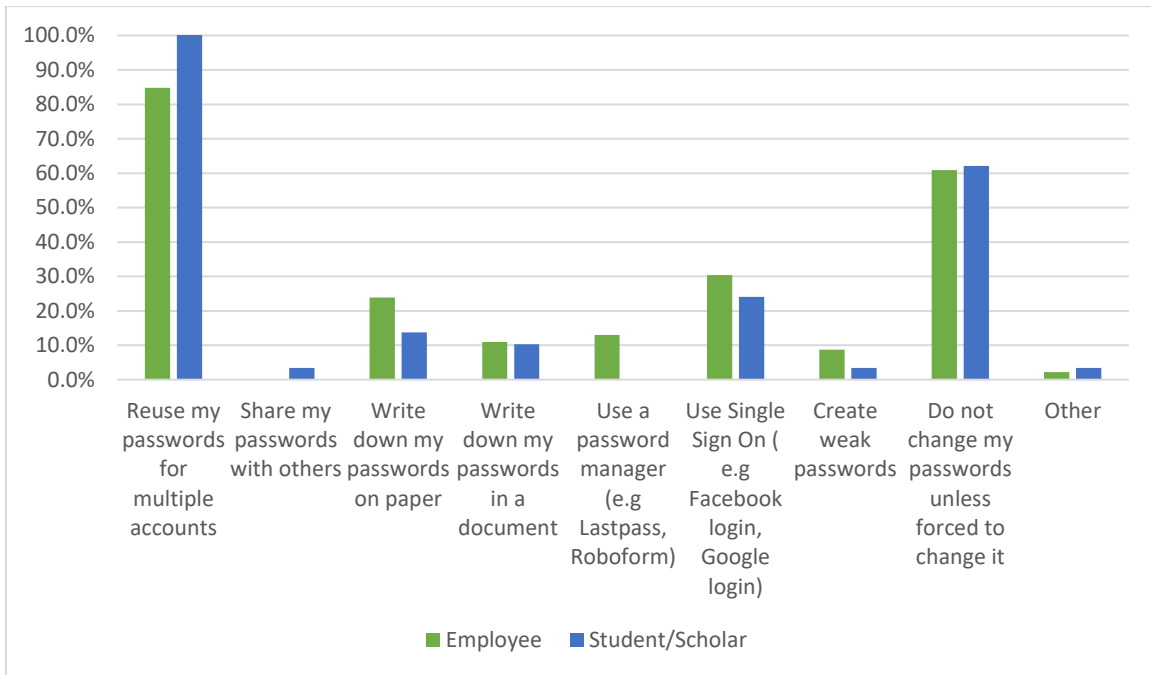


Figure 6.12: Question 3.5 Results

Question 3.5 asked the respondents which coping strategies they usually adopt. From Figure 6.12 it can be determined that the two groups had adopted similar coping strategies. However, there were some slight differences such as the 23.9% of employees who *'Write down my passwords on paper'* compared to 13.7% of the student/scholar group. With regard to *'Use a password managers'* coping strategies, 13.0% of employees used password managers whereas 0.0% of student/scholars did.

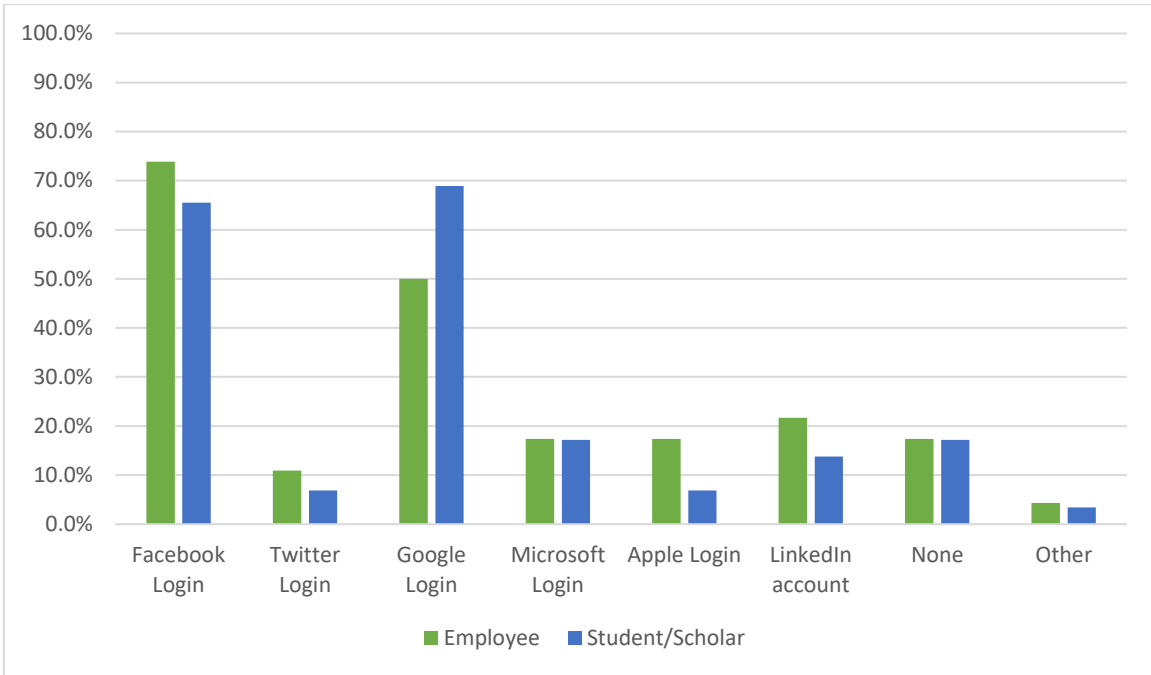


Figure 6.13: Question 3.6 Results

Question 3.6 asked the respondents which Single Sign-On they use. From Figure 6.13, it can be determined that the two groups commonly use the same Single Sign-On login. However, there were some slight differences such as 68.9% of the student/scholar group used Google Login compared to the 50.0% of the employees group. 17.4% of the employee group used Apple login compared to 6.9% of the student/scholar group.

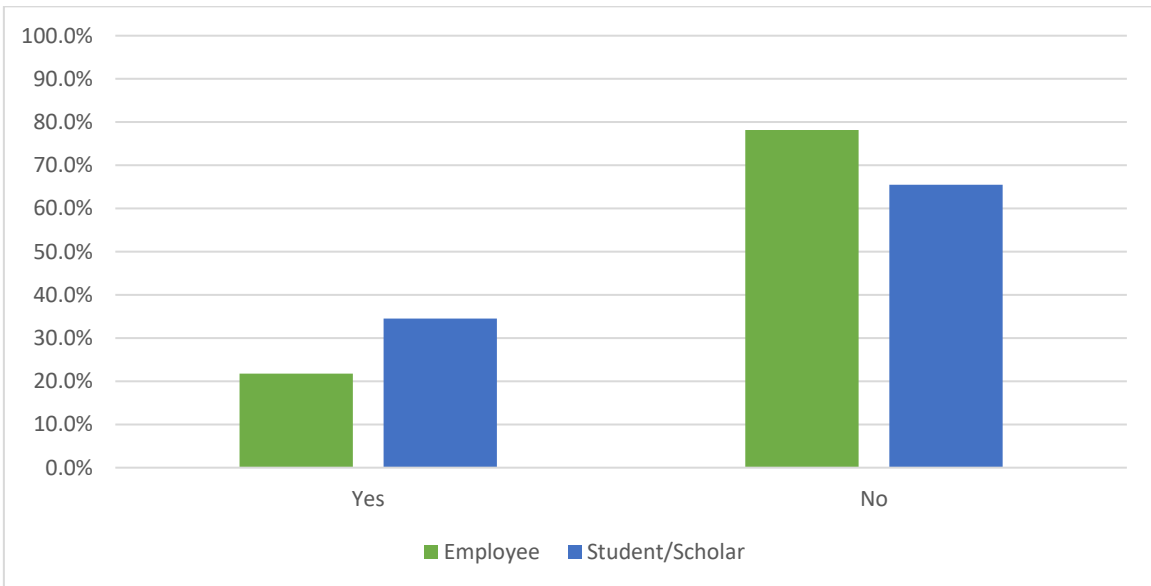


Figure 6.14: Question 3.7 Results

Question 3.7 asked the respondents if they had attended an awareness or educational programme on passwords. From Figure 6.14, it was identified that 34.5% respondents in the student/scholar group had attended password awareness or educational programmes compared to 21.8% of employees. As mentioned previously, this question was expanded into another question to determine where the respondents attended password awareness or educational programmes. Figure 6.5 below presents the results of where the respondents attended password awareness or educational programmes.

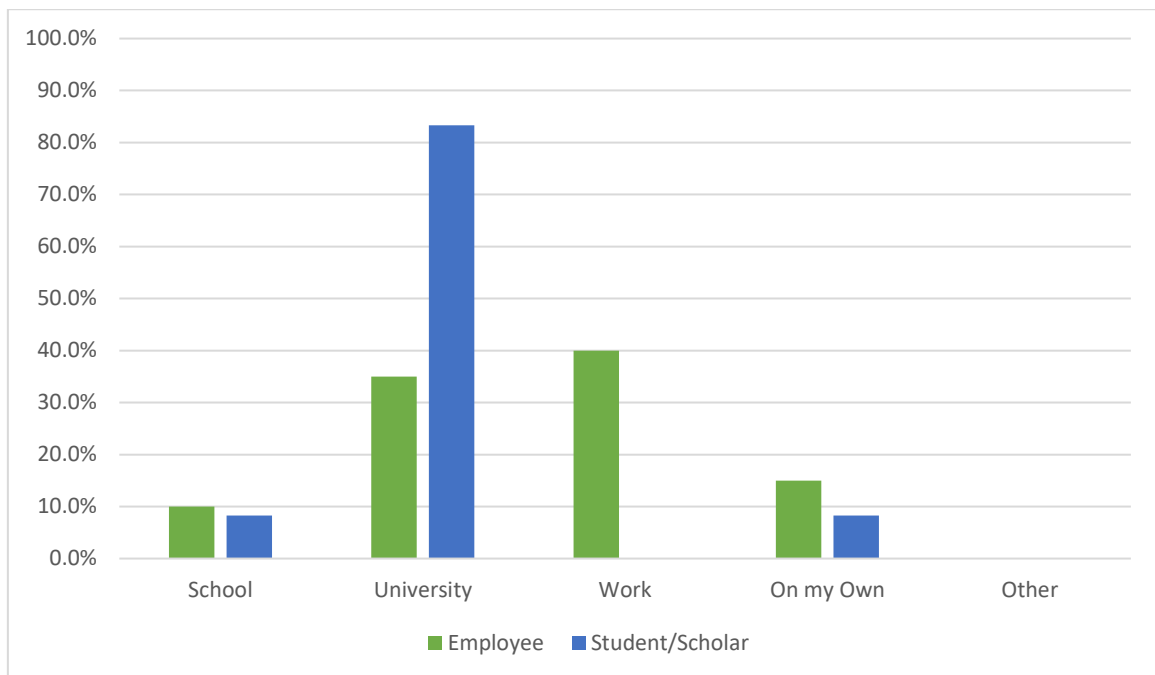


Figure 6.15: Question 3.7a Results

From Figure 6.15 it can be seen that the students attended password awareness or educational programmes mostly at university. For employees who attended awareness or educational programmes, these programmes were conducted at their workplace. However, the fact that not many employees have attended an awareness or an educational password programme, is of concern. If employees have not been part of an awareness or educational programme, they could adopt insecure password management behaviours.

Both the employee and student/scholar groups state that they are satisfied about the prescribed password minimum length being 8 characters, whereas for the maximum password length of 16 characters, the student/scholar group felt more neutral about this guideline compared to the employee group, which felt more

satisfied. Both groups reported that the maximum password length of 16 characters would be more secure. However, respondents in both groups stated that it is too long and would be difficult to remember. With regard to the composition requirements, both groups were of the opinion that passwords should contain composition requirements. However, many respondents still found the composition requirements to be burdensome, even though they agreed it should be there. The sample password policy states that passwords must be changed every 90 days. In this regard, employees and the student/scholar group stated that they prefer to never change their passwords at all. This result is not surprising as users tend to find the changing of passwords frustrating. With regard to the general password recommendations from the policy, the employee and student/scholar groups agreed that the recommendations were helpful in providing better protection for their passwords. As seen from Figure 6.6, there were more employees who agreed that the general password recommendations were helpful compared to the student/scholar group. The employee group and the student/scholar group both stated that the sample password policy would generally not be difficult to adhere to. However, they found the Password Maintenance section of the policy to be difficult to adhere to.

With regard to the behaviour and coping strategies of both groups, it was found that there were slight differences between the groups. Both groups stated that they often use the same password for different accounts because they do not want to remember multiple passwords and find it difficult to remember multiple passwords. With regard to Password Generation, both employee and student/scholar groups stated that they make minor change(s) to an existing password, use existing passwords from other accounts or use Single Sign-On login, if available. Both student/scholar and employee groups re-use passwords across many accounts, as this coping strategy is quite common. In order for employees and students to keep track of their passwords, they rely heavily on memorising their passwords, using the “forgot password” feature, using Single Sign-On and writing down their passwords on paper. The coping strategies that the two groups commonly adopt are:

- Reuse my password across multiple accounts
- Never change my passwords unless forced to

- Single Sign-On
- Writing passwords down on paper

From the questionnaire it was found that both groups find the Password Maintenance section difficult to adhere to because it requires the user to change their passwords every 90 days. With regard to Password Management behaviour, it was found that password re-use was the most common coping strategy used among employees and students/scholars, as they do not want to remember multiple passwords and find it difficult to remember multiple passwords. When respondents create passwords, they often make minor changes to an existing password or use the Single Sign-On. One of the results that really stood out, was the education and awareness programmes related to passwords because the majority of employees have not been part of an awareness or educational programme with regard to passwords. This is of serious concern because if employees have not been part of an awareness or educational programme, they could adopt insecure password management behaviours and not know the importance of password security and its consequences.

6.6 Conclusion

This chapter summarised the general results and findings from the questionnaire. The results and findings of the questionnaire were divided into three sections, namely the Demographic Results, Sample Password Policy and Behaviour and Coping Strategies. A total of 75 respondents completed the survey. The findings from the survey pointed out that the Password Maintenance section of the Sample Password Policy was the most difficult section for users because they struggled to adhere to it. However, the respondents overall did not find the Sample Password Policy difficult to adhere to.

In addition, the coping strategies identified from the survey correlate with the literature as seen in Chapter 4, Section 4.3. From the survey it was identified which coping strategies were commonly used amongst respondents, ranging from the most used to the least used, namely Reusing Passwords, Not Changing passwords, Single Sign-On and Writing Down Passwords.

This chapter helped determine users' perceptions towards password policies and identified users' coping strategies with regard to password policies. The following chapter interprets the results of user perceptions towards the NIST SP 800-63B (2016).

Chapter 7 : Interpretation and Discussion

The aim of this chapter is to interpret the results from the questionnaire by highlighting those results pertaining to the NIST SP 800-63 (2016) and determining users' perceptions towards this new standard.

7.1 Introduction

The previous chapter presented the general results and findings from the questionnaire. It also identified users' coping strategies when trying to adhere to password policies. This chapter focuses primarily on the results from the questionnaire, which related to the NIST SP 800-63B (2016) password guidelines. The new guidelines of the NIST SP 800-63B (2016) were presented in Chapter 3, Section 3.2.4, and were integrated into the questionnaire to determine users' perceptions towards them.

This chapter is structured as follows: Section 7.2 compares the NIST SP 800-63B (2016) to the NIST SP 800-63B (2017). Section 7.3 presents the respondents' perceptions related to the common password policy elements, while Section 7.4 presents the results and findings pertaining to perceptions of the NIST SP 800-63B (2016). Section 7.5 discusses the perceptions of NIST SP 800-63B (2016), while Section 7.6 presents the password policy recommendations. Section 7.7 concludes this chapter.

7.2 NIST SP 800 63B (2016) and NIST SP 800 63B (2017)

This research study initially referred to the DRAFT NIST Special Publication 800 63B (NIST SP 800-63B, 2016) *Digital Identity Guidelines Authentication and Lifecycle Management* during the initial literature review and design of the questionnaire. The new NIST Special Publication 800 63B (NIST SP 800-63B, 2017) *Digital Identity Guidelines Authentication and Lifecycle Management* was accepted in June 2017. This standard was studied to determine whether there had been any major changes from the draft publication. With regard to the sections of the NIST SP 800-63B (2016) which were used to develop the questionnaire, minor changes from the draft to the accepted standard were identified. These changes are presented in Table 7.1

NIST SP 800-63B (2016)	NIST SP 800-63B (2017)
Verifiers SHOULD permit user-chosen memorised secrets to be up to 64 characters or more in length.	Verifiers SHOULD permit subscriber-chosen memorised secrets at least 64 characters in length
Verifiers SHOULD NOT impose other composition rules (e.g., mixtures of different character types) on memorised secrets.	Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorised secrets.
Verifiers SHOULD NOT require memorised secrets to be changed arbitrarily (e.g., periodically) and SHOULD only require a change if the subscriber requests a change or there is evidence of compromise of the authenticator.	Verifiers SHOULD NOT require memorised secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.

Table 7.1: NIST SP 800-63B(2016) and NIST SP 800-63B(2017)

The small differences from the draft to the accepted standard included different words, such as the draft uses the term “user-chosen memorised secret”, whereas the NIST SP 800-63B (2017) uses the term “subscriber-chosen memorised secret”. In the draft it stated that “*Verifiers SHOULD permit user-chosen memorised secrets to be up to 64 characters or more in length*”, which means that password-based authentication systems should allow passwords up to 64 characters or more in length to support the use of passphrases. However, the NIST SP 800-63B (2017) states that “*Verifiers SHOULD permit subscriber-chosen memorised secrets at least 64 characters in length*”. This means that systems should allow passwords of at least 64 characters in length. This can be misleading when relating it to minimum and maximum password length requirements. With regard to the composition rules, both standards have the same guideline. However, the NIST SP 800-63B (2017) added that repeated consecutive characters would be prohibited. Both standards state that password-based authentication systems should only force users to change passwords if there is evidence of compromise. However, the NIST SP 800-63B (2016) stated that users could change their passwords upon request, whereas the NIST SP 800-63B (2017) does not suggest this.

In conclusion, there were no major changes from the NIST SP 800-63B (2016) to the NIST SP 800-63B (2017).

7.3 Perceptions of Common Password Policy Elements

Chapter 4, Section 4.2, discusses how the password policy common elements: (Password Length, Password Complexity, Password Expiration, Password History, and Password Protection) impact human memory. These elements are related to memory limitations.

Table 7.1 depicts the respondents' perceptions towards the common password policy elements of the Sample Password Policy. The detail refers to the password guidelines which come from the Sample Password Policy. This section focused only on the elements which were of concern, in order to determine why respondents felt that way towards the password guideline.

PERCEPTIONS OF COMMON ELEMENTS OF PASSWORD POLICIES		
Common Elements	Detail	General Perceptions
Password Length	Minimum password length of 8 characters	Generally accepted
	Maximum password length of 16 characters	Some concerns
Password Complexity	Passwords must contain 3 of the following types: lowercase, uppercase letters, numbers and special characters	Generally accepted
Password Expiration	Password must be changed every 90 days	Some concerns
Password History	Users must not reuse previous passwords	Generally accepted
Password Protection	Do not use the "Remember Password" feature of applications	Generally accepted
	Do not store passwords in a file on any computer system unencrypted	
	Ensure you do not allow someone to see you type in your password (shoulder surfing)	

Table 7.2: Perceptions Towards Sample Password Policy

With regard to the password length element there was concern about the maximum password length of 16 characters. The respondents from the survey were generally dissatisfied about this specific guideline and mentioned that, although their

passwords would be harder to crack, if their password was between 8 and 16 characters it was still too long and harder to remember. The Password Expiration requested that users change their password every 90 days. From the survey it was determined that the most difficult aspect (section) of the Sample Password Policy was the 'Password Maintenance', section which consists of the Password Expiration element. The respondents stated that they would prefer to never have to change their passwords, because they *'find it difficult having multiple passwords and having to create a new one every few months/weeks'*

The coping strategies identified from the survey that were commonly used amongst the users were: Re-using passwords, Not changing passwords, Single Sign-On, Writing down passwords, Password managers and Creating weak passwords. The coping strategies identified from the survey align with the literature, as seen in Chapter 4, Section 4.3. Based on the literature, Password Length, Password Complexity, Password Expiration, Password History and Password Protection have an impact on memory and could result in users adopting certain insecure coping strategies. Therefore, policy makers should consider whether certain common password policy elements should be part of their password policy, as they have a severe impact on human memory. To help policy makers, NIST has come up with new guidelines for password-based authentication. In the new standard, the guidelines for the common elements of Password Complexity, Password Expiration and Password History have changed.

The following section presents the respondents perceptions towards the new password-based authentication guidelines in the NIST SP 800-63B (2016).

7.4 NIST SP800-63B Results and Findings

Chapter 3, Subsection 3.2.4, discusses the new NIST guidelines for password-based authentication systems and password requirements. This section highlights each NIST guideline from the new standard, together with the survey question which links to the specific NIST guideline, in order to determine users perceptions towards these new guidelines.

NIST SP 800-63B (2016) 5.1.1.2	Survey Related Question
Verifiers SHALL require user-chosen memorised secrets to be at least 8 characters in length	2.1 How do you feel about the prescribed password minimum length being 8 characters (Section 4.1.1)?

Table 7.3: Minimum Password Length

The NIST guideline in Table 7.3 stipulates that passwords shall be at least 8 characters in length. The respondents indicated that they were generally satisfied with the minimum length being 8 characters.

NIST SP 800-63B (2016) 5.1.1.2	Survey Related Question
Verifiers SHOULD permit user-chosen memorised secrets to be up to 64 characters or more in length	2.3 How would you feel if passwords maximum prescribed length was increased to 64 characters?

Table 7.4: Maximum Password Length

Section 10.2.1 mentions that when users create passwords, the verifiers should allow at least 64 characters in length to support the use of passphrases. In Table 7.4 this means that there is a limit on the maximum password length of at least 64 characters in length. Respondents indicated that they would be dissatisfied if the maximum password length was increased to 64 characters. Although respondents stated that this would be more secure, they also mentioned that it would be *'too long to remember'* and they could make *'typing errors'*. As mentioned previously in Chapter 6, Section 6.3, there was some confusion with this question, as some users thought that their passwords would have to be 64 characters in length

NIST SP 800-63B (2016) 5.1.1.2	Survey Related Question
Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets	2.4 Do you feel that passwords should have composition requirements as outlined in Section 4.1.3?

Table 7.5: Password Composition Requirements

Table 7.5 indicates that, although the NIST guideline states that password-based authentication systems should not impose composition rules, the respondents were of the opinion that passwords should have composition requirements.

NIST SP 800-63B (2016) 5.1.1.2	Survey Related Question
All printing ASCII characters as well as the space character SHOULD be acceptable in memorised secrets.	2.5 Would you like the option of using spaces and emoji's (smiley face 😊,sad face ☹) in your passwords?

Table 7.6: ASCII Characters

With regards to this guideline as per Table 7.6, the users had mixed feelings towards this. The results were split equally, with respondents liking the option of using spaces and emoji's in passwords and others not.

NIST SP 800-63B (2016) 5.1.1.2	Survey Related Question
Verifiers SHOULD NOT require memorised secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authentication.	2.6 How often would you prefer to change your passwords?

Table 7.7: Password Expiration

With regard to Table 7.7, the NIST guideline states that password-based authentication systems should not require users to change their passwords periodically. From the survey, the respondents preferred to never have to change their passwords.

NIST SP 800-63B (2016) 5.1.1.2	Survey Related question
Verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised	2.8 Would you prefer to have your chosen password automatically checked by the system against a list of commonly breached/hacked/compromised passwords before committing to it?

Table 7.8: System Checking of Passwords

The guideline in Table 7.8 recommends that users' passwords be checked against a list of commonly-used or compromised passwords. The respondents mostly had positive attitudes towards accepting this new guideline, which would have a positive impact on the creation of more secure passwords.

The following section discusses the users' perceptions towards the new NIST guidelines in more detail.

7.5 Discussion of NIST SP 800-63B (2016)

Table 7.9 depicts the respondents' perceptions towards the new NIST SP 800-63B (2016). The general perception details refer to the password guidelines which come from the NIST SP 800-63B (2016) standard.

Common Elements	NIST Detail	General Perception
Password Length	Minimum password length of 8 characters	Generally accepted
	Maximum password length of 64 characters or more	Some concerns
Password Complexity	Do not force composition change	Some concern
Password Expiration	Not force passwords to be changed periodically	Generally accepted
Password History	Does not mention anything about keeping a record of users previously used passwords	Not applicable
Password Protection	Checking passwords against a list of commonly/compromised passwords	Generally accepted

Table 7.9: Perceptions Regarding NIST SP 800-63B (2016)

With regard to the Password Length element, there was some concern with the maximum password length of 64 characters. The respondents from the survey were generally dissatisfied about this specific guideline and mentioned that, although it would make their passwords more secure, it was too long, prone to typing errors and harder to remember. Although NIST implemented the increase in maximum password length with the aim of making the password more secure, it could be argued that general users battle to remember their current passwords of 16 characters in length. There was some concern with the Password Complexity as the respondents were of the opinion that their passwords should contain composition requirements. It can be argued that the respondents believed that having complex passwords is more secure, so they were in agreement that Password Complexity is required. The respondents were probably under the impression that complex passwords is the only way for a password to be secure.

7.5.1 Password Length

Password Length referred to a minimum prescribed length of 8 characters and a maximum prescribed length of 64 characters or more. The respondents indicated that they were satisfied about the minimum length requirement of 8 characters. With regard to the maximum prescribed length, the respondents were not satisfied with this guideline, as they stated that it was *“Too long and would be easily forgotten”* and *“not easy to remember”*. Although the respondents were aware that 64

characters would be more secure, they believed that they would not be able to remember such long passwords.

7.5.2 Password Complexity

Password Complexity did not require passwords to contain composition requirements. It is a known fact that users generate weak passwords when trying to comply with password policy requirements. In this regard, NIST aims to make password generation easier for the user, while making sure the password is secure. This could be the reason NIST suggests that password-based authentication systems should not force composition rules, but rather favour longer passwords. This would make the password easier for the user, while still being secure. With regard to using ASCII characters, such as spaces and emoji's in their passwords, it was found that the respondents had mixed feelings. Half of the respondents indicated that they would like this option and the other half stated that they did not like this option. The positive impact that this guideline has, is that it does not force users to use ASCII characters, but rather gives them the option of using these characters in their passwords. NIST states that using spaces could introduce usability issues. However, it may be beneficial to remove repeated spaces from passwords prior to verification (NIST SP 800-63B, 2016). This is a good recommendation, as users may mistype or add an extra space by mistake. Therefore, it would be good to remove repeated spaces before the user commits to the password.

7.5.3 Password Expiration

Password Expiration states that users should not be forced to change their passwords periodically. The respondents stated that they prefer to never have to change their passwords. The results from the questionnaire indicate that the respondents have a positive attitude towards the new guideline, which states that password-based authentication systems should not force users to change their passwords periodically. Instead, changes should be made at the user's request or if there is evidence of the password being compromised. The Password Expiration element was perceived to be a source of frustration for users, as this would force users to generate new passwords after a certain number of days. Many users would not change their passwords even though the password had passed its expiration period.

7.5.4 Password Protection

Password Protection checks users' newly created passwords against a list of commonly-used or compromised passwords before users commit to it. This specific guideline was generally accepted among the respondents and the respondents stated that:

- *'Would reduce the risk of passwords being compromised'*;
- *'Feel reassurance that their password is secure and safe'*;
- *'Help create stronger passwords'*

Many users may think that their password is strong and secure, when it is, in fact, the complete opposite. So this guideline would also make users more aware about the security of their passwords that is, whether it is secure or not, or whether it is a commonly used or compromised password.

From the survey it was found that, based on the users' perceptions, they were of the opinion that password policies should have a minimum password length of 8 characters. This is in line with the NIST requirements that "*Verifiers SHALL require subscriber-chosen memorised secrets to be at least 8 characters in length*" and "*Verifiers SHOULD permit subscriber-chosen memorised secrets to be up to 64 or more characters in length*". The users were of the opinion that passwords should contain composition requirements and that their passwords could contain ASCII characters such spaces and emoji's. NIST states that "*Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorised secrets*" and "*All printing ASCII characters as well as the space character SHOULD be acceptable in memorised secrets*". NIST clearly states that the composition requirements should not be forced upon the users, unlike the previous standards which forced the passwords to have composition requirements. The respondents' perceptions towards the Password Expiration is that they felt they should not have to change their passwords ever. This perception aligns with the new NIST guideline which states that "*Verifiers SHOULD NOT require memorised secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authentication*". The respondents perceived that

checking passwords against a list of commonly used/compromised passwords was helpful and secure. Once again this aligns with what NIST aims to do by “*Verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised*”. From the survey it can be determined that the users mostly prefer the new password guidelines imposed by NIST.

With regard to users’ perceptions towards the new NIST guidelines on passwords, they perceived these guidelines to be helpful, secure and easier to adhere to. These new guidelines implemented by NIST addressed the usability issues users had with common elements of password policies, such as the password composition rules and Password Expiration. Previous research has shown that users often found the composition requirements to be annoying and burdensome. Therefore, NIST changed the ‘Password Composition’ element. Often when users create their passwords, there would be some pattern with regard to the composition rules, such as adding an exclamation mark “!” at the end of the password or replacing certain letters with special characters, for example, replacing the a with an @ (Ur et al., 2015). Users typically make use of these coping strategies when creating passwords to aid them with the difficulty of remembering too many passwords. NIST took this into consideration by eliminating the composition rules and encouraging password-based authentication systems to accept longer passwords.

As seen from previous research, users often do not like the Password Expiration element. The same finding was obtained from the survey where the respondents stated that they would prefer to never change their passwords. Although forcing users to change their passwords to prevent attackers from guessing them, often the new password is still predictable since users commonly only make minor modifications to the old one (Florêncio et al., 2014a). So NIST took the Password Expiration issue into consideration and decided to change the Password Expiration, thus making it easier for the user in that they do not have to create and remember new passwords. Passwords can be changed upon the user’s request or if there is evidence of the password-based authentication system having been compromised.

Furthermore password-based authentication systems should not force the users to use composition and ASCII characters. However, users can determine their own

Password Complexity. In addition the password-based authentication system should check users' passwords against a list of commonly compromised passwords as the respondents stated that this would help create stronger passwords and give them reassurance regarding the security of their passwords. Lastly the password-based authentication system should allow passwords to be a minimum of 8 characters while allowing a maximum of 64 characters or more in length. The respondents found these NIST guidelines to be helpful, secure and easier to adhere to.

The following section recommends the elements that should be included in a password policy.

7.6 Password Policy Recommendations

Table 7.10 summarises the elements to be considered when revising existing password policies or creating new password policies.

Common Element	Recommendation
Password Length	Minimum length of 8 characters
	Maximum length of up to 64 or more characters
Password Complexity	Should not force users to use composition requirements
Password Expiration	Should not force users to change their passwords periodically instead by the user's own choice or evidence of the password being compromised.
Password History	Password-based authentication should keep a record of previously used passwords
Password Protection	Checking passwords against a list of commonly-used or compromised passwords before the user commits to it.

Table 7.10: Password Policy Recommendations

The elements recommended here are based on the results of the survey and the related user perceptions regarding these elements.

7.6.1 Password Length

With regard to Password Length, if the minimum Password Length is too long, then the users would have problems remembering their passwords. The users could also feel annoyed and frustrated if the maximum password length is too long. The recommended prescribed minimum Password Length should be set to 8 characters in length. This is in line with best practice, which recommends a minimum of 8 characters, as seen from the NIST SP 800-63B (2016) and Microsoft, Apple and Google. Providing a minimum Password Length of 8 characters provides sufficient

security and is still easy for the user to remember. The prescribed maximum Password Length should be set to 64 characters or more. This will provide freedom to the users who prefer to use longer passwords, such as passphrases, as they will not be restricted. Some users may find passphrases easier to remember than shorter passwords, which could improve their attitude towards password security.

7.6.2 Password Complexity

The password-related standards and best practices such as ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013) and SANS Password Protection Policy (2014b), often forced the users to use password composition requirements in their passwords. When users are forced to use password composition requirements, they would often find this guideline to be burdensome and annoying. The recommendation is that password-based authentication systems should not force users, but rather give users the option of using composition requirements in their passwords, as the Password Complexity element often affects the user's memory. The password-based authentication systems should also accept ASCII characters such as spaces and emoji's. These recommendations align with the new NIST SP 800-63B standard (2016), which states that password-based authentication systems should not force users to use composition requirements in their passwords.

7.6.3 Password Expiration

Password-related standards and best practices, such as ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013) and SANS Password Protection Policy (2014b), would force the users to change their passwords after a certain number of days. When password-based authentication systems force users to change their passwords, it often causes frustration, which could lead users to adopt certain insecure coping strategies, such as Re-using Passwords or Creating Weak Passwords. Thus, the recommendation is that password-based authentication systems should not force users to change their passwords periodically. The Password Expiration affects the human memory limitations because users have to create new passwords after a certain number of days and remember those new passwords. This could negatively affect users' attitudes towards password security. Therefore, NIST suggested that password-based authentication should not force users to change their passwords periodically. However, the user's password can be

changed upon the user's request or if there is evidence of the password having been compromised.

7.6.4 Password History

The password-related standards and best practices, such as ISO/IEC 27002 (2013) and NIST SP 800-118 (2009), state that the password-based authentication system must maintain a record of previously used passwords to prevent the reusing of passwords. However, NIST SP 800-63B (2016) does not mention anything with regard to Password History. It could be argued that the reason why it is not mentioned is due to the fact that password-based authentication systems should no longer require users to change their passwords periodically. However, the recommendation is to include the Password History as it would prevent Reusing Passwords for the same account.

7.6.5 Password Protection

The Password Protection element recommends that the user's password must be checked against a list of commonly used or compromised passwords. This would prevent users from generating predictable passwords, in order to better protect their information. This recommendation aligns with the NIST SP 800-63B (2016).

As mentioned previously the Password Complexity, Password Expiration and Password History guidelines have changed from the NIST SP 800-63B (2016). However, Table 7.9 recommends that Password Complexity and Password Expiration be included in password policies. In previous standards and best practices these elements were mandatory and forced upon the users, whereas now the users can use composition requirements and even change their passwords if they choose to do so.

7.6.6 Password Coping Strategies

With regard to Password Coping Strategies, not all coping strategies are considered to be insecure, for example, the use of Single Sign-On and Password Managers. ISO/IEC 27002 (2013) and NIST SP 800-18 (2009) suggest that Single Sign-On can be used as an alternative to reduce the limitations of human memory, as users normally have to remember multiple passwords. The standards and best practices do not mention anything with regard to Using Password Managers. The

recommendation would be that users must consider the use of Single Sign-On to overcome the human memory limitation.

7.7 Conclusion

The aim of this chapter was to interpret and discuss the survey results which focused on the new NIST SP 800-63B (2016). The respondents' perceptions of common password policy elements were identified in relation to the sample password policy. It was determined that the maximum password length of 16 characters and Password Expiration were difficult for the user.

The respondents' perceived the new NIST SP 800-63B (2016) was perceived to be helpful, secure and easier to adhere to. It was found that there were some concerns with the Password Length and Password Complexity elements of the new NIST standard. Password Policy Recommendations were presented for organisations that are wanting to revise existing password policies or creating new password policies. These were based on the results of the survey conducted and the related respondents' perceptions regarding these elements.

In conclusion, the new guidelines in the NIST SP 800-63B (2016) were perceived to be helpful, secure and easier to adhere to. The following chapter concludes the research study.

Chapter 8 : Conclusion

This chapter concludes the research study by drawing conclusions based on the research presented in the previous chapters. It also mentions how the aims of the chapters were accomplished, by providing a summary of each chapter. In addition, this chapter states how and where in the dissertation each of the primary and secondary research objectives were met. Furthermore, it highlights the main contribution of this research, as well as the research limitations and recommendations for future research.

8.1 Introduction

Information is important to the well-being of all organisations and, therefore, needs to be protected against various threats and unauthorised access. Identification and authentication are commonly used to help ensure the confidentiality, integrity and availability (CIA) of information assets. This research study focused on password-based authentication. When creating a password, users often have to adhere to a password policy, which is typically developed from password-related standards and best practices. This implies that, before organisations implement password guidelines, they need to determine users' perceptions towards such guidelines.

The problem stated in Chapter 1, Section 1.2, that this research aimed to solve is ***Organisations often implement password policy guidelines without taking into consideration users' perceptions regarding such guidelines. This could result in users adopting various password management coping strategies.*** To address this problem, it was necessary to understand users perceptions regarding current password policy guidelines (standards and best practices).

Section 8.2 of this chapter provides a summary of the previous chapters that were used to address the above-mentioned problem. Section 8.3 discusses how the research objectives, outlined in Chapter 1, were met. Furthermore, Section 8.4 states the research contribution and Section 8.5 outlines the research limitations of this research study. Section 8.6 provides suggestions for future research and Section 8.7 concludes this research study.

8.2 Summary of Chapters

Chapter 1 aimed to introduce information security as the research area in which this research is situated and to identify a problem within information security. The problem identified was in the specific field of password security. In order to address the problem, certain research objectives were established. This chapter set out the various research methods that were used to meet the identified research objectives.

Chapter 2 aimed to help the reader understand the importance of passwords by conducting a content analysis, which also helped to determine specific themes within password-related literature. The consequences of poor password security were presented, as well as the McCumber model, which provides a security measures to improve the protection of an organisation's information assets. The alternative methods to replace passwords were presented, together with the advantages and disadvantages of each. Although alternative methods have been considered to replace passwords, most systems today still use password authentication. This chapter shows that a password goes through a lifecycle of '*Password Generation*', '*Password Maintenance*' and '*Password Authentication*' (Refer to the password management lifecycle in Chapter 2, Section 2.2.3). The common elements of password policies were identified which included Password Length, Password Complexity, Password Expiration, Password History and Password Protection and were further discussed in Chapter 3. This chapter argued that passwords are not going to disappear anytime soon, as it still remains the most cost-effective and efficient method to control access.

Chapter 3 focused on the *Policy and Practice* security measure of the McCumber model and introduced the password-related standards and best practices, such as ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2(2013), NIST SP 800-63B (2016) and SANS Password Protection Policy (2014b). Furthermore, the chapter discussed each standard and best practice regarding what they emphasise about passwords, and identified the common elements of password policies. In addition, a comparison was done in order to determine the differences between some of the old and new NIST standards. The structure of the password policy was presented by stating what the password policy should include, as well as the common elements that were identified.

Chapter 4 focused on the *Human Factor* security measure of the McCumber model. This chapter aimed to identify the human factors and coping strategies with regard to password management. Furthermore, it aimed to determine how the common elements of password policies could affect human factors, such as memory, attitude and apathy. This was presented in Section 4.2. The chapter also aimed to determine how memory, attitude and apathy could affect the users behaviour regarding password management. This was discussed in Section 4.3. In addition, this chapter argued that one of the ways of addressing the attitude and apathy aspect, is through education, training and awareness programs. Various coping strategies were identified such as reusing password, writing down of passwords, creating weak passwords, not changing passwords and using Single Sign-On and password managers. However the use of Single Sign-On is not considered a bad coping strategy as some standards suggest Single Sign-On as authentication. These were used to evaluate how the standards and best practices attempt to prevent the adoption of such coping strategies.

Chapter 5 aimed to introduce the research approach and research methods that were followed in conducting this research study. This chapter presented the sampling technique which was used to target the respondents for the survey, as well as the design of the questionnaire.

Chapter 6 aimed to present the results and findings from the survey. The results and findings were presented and discussed according to the sections of the questionnaire, namely: Demographics, Sample Password Policy and Behaviour, and Coping Strategies. Furthermore, a comparison was made between the scholar/student group and the employee group in order to determine if there were any differences between the two groups. These results are presented in Section 6.5.

Chapter 7 aimed to interpret the results from the survey regarding the new NIST password guidelines. It argued that some common elements affect the human memory. Policy makers need to take into consideration which elements should be part of the password policy. In addition, the new NIST standard helps with decisions regarding password policies. However, users' perceptions towards this standard still needed to be determined. The respondents' results, which focused on the new NIST

password guidelines, were presented and discussed to determine how the respondents perceived the new NIST standard. It was discovered that the respondents found the new NIST password guidelines to be helpful, secure and easier to adhere to. Lastly, based on the respondents' perceptions, this chapter identified specific guidelines that need to be considered when developing or revising a password policy. These guidelines generally correlated with the new NIST SP 800-63B (2016).

8.3 Meeting the Research Objectives

The primary objective of this research study was, *To determine users' perceptions regarding key elements of current password policy guidelines*. In order to meet this primary objective, three secondary objectives were established. The secondary objectives are restated and described below. Meeting the identified secondary objectives contributed towards achieving the primary objective.

Secondary objective 1 aimed to determine the key elements of current password policy guidelines.

In Chapter 3, this objective was met through focusing on the various password-related standards and best practices, which were the ISO/IEC 27002 (2013), NIST SP 800-118 (2009), NIST SP 800-63-2 (2013), NIST SP 800-63B (2016) and SANS Password Protection Policy (2014b). These specific standards and best practices were chosen because they relate to password guidelines and many organisations rely on standards and best practices when developing their password policies. For each standard and best practice, certain sections were considered to be most relevant in terms of this research study and were focused on in order to determine the common elements of each. Upon reviewing each standard and best practice, it was found that there were certain commonalities between them. These commonalities are referred to as common elements. The common elements that were identified, were Password Length, Password Complexity, Password Expiration, Password History and Password Protection. Furthermore, it was argued that those elements need to be included in password policies.

Secondary objective 2 aimed to determine human factors and coping strategies relating to password management.

This objective was met in Chapter 4 where the human factors that relate to password management were identified. The human factors included the human memory limitations, attitude and apathy, which are discussed in Section 4.2. Furthermore, it was argued that the common elements, identified in Chapter 3, have an impact on the human memory and on the attitude and apathy of users, and that these human limitations could force users to adopt certain insecure coping strategies. The coping strategies related to password management were identified and included the following: Reusing Passwords, Writing Down Passwords, Creating Weak Passwords, Not Changing Passwords and using Single Sign-On and Password Managers. Furthermore, it was argued that human limitations could result in users adopting certain coping strategies, which are presented in Section 4.3.2. In addition, education, training and awareness programmes regarding passwords are recommended to address some of the human factors that were identified

Secondary objective 3 aimed to evaluate current password policy guidelines with regard to coping strategies.

This secondary objective was met in Chapter 4. Once the coping strategies were identified in Section 4.3, the standards and best practices were evaluated in order to determine how they attempt to prevent the users from adopting certain insecure coping strategies. It was discovered that the standards and best practices attempt to prevent the creation of weak passwords by stipulating that passwords have both a minimum length and composition requirements. With regard to the writing down of passwords, the standards and best practices state that users should not write down passwords. However, ISO/IEC 27002 (2013) allows users to write down passwords, as long as the password is stored securely and adheres to the password policy. ISO/IEC 27002 (2013) and NIST SP 800-118 (2009) attempt to prevent the re-use of passwords by keeping a record of previously used passwords. The SANS Password Protection Policy (2014b) states that users must not use the same password for both company accounts and non-company accounts. Some of the standards and best practices attempt to prevent users from not changing passwords, by forcing passwords to be changed after the expiration period. ISO/IEC 27002 (2013) and NIST SP 800-118 (2009) both state that Single Sign-On can be used instead of a login process.

8.4 Contribution of Research

The primary objective of this research study was to determine users' perceptions regarding key elements of current password policy guidelines.

The primary objective was met in Chapters 6 and 7 where the results and findings were presented and discussed. The results were interpreted in order to understand the users' perceptions regarding the key elements of current password policy guidelines. From the survey it was determined that Password Length and Password Expiration were the elements that respondents found most difficult to adhere to. With regard to the Sample Password Policy, which was part of the survey, the respondents generally did not find it difficult to adhere to. The results of the survey were interpreted in Chapter 7, Section 7.4, in order to understand the respondents' perceptions towards the new NIST password guidelines. The respondents found the new NIST password guidelines to be helpful, secure and easier to adhere to. Finally Password Policy Recommendations were presented in Chapter 7, Section 7.6 based on the respondents' perceptions towards the new NIST standard and results of the survey.

8.5 Research Limitations

The limitations of this research study was that it only had a total of 75 respondents for the survey.

The survey results and findings are based on the respondents that responded and cannot be generalised to all users' perceptions regarding password policies.

8.6 Suggestions for Future Research

Future research could distribute the same survey to a different context, for example within small and large organisations. The respondents would be employees of the target companies and the research could include a comparison between the perceptions of employees at small companies versus the perceptions of employees at large organisations.

Another suggestion for future research is to determine how the human factors, such as memory, attitude and apathy affect users' coping strategies, by going into more detail as to why users adopt certain coping strategies and not others. This could be done through interviews or focus groups.

8.7 Epilogue

The process undertaken to complete this research study has been immensely fulfilling and a great learning experience. Before organisations implement password policy guidelines, they need to understand users' perceptions towards current password policy guideline. It is envisaged that the results and findings may help organisations to better understand users' perceptions towards password policies. The Password Policy Recommendations provides a starting point for organisations revising existing or implementing new password policy guidelines

References

- Abie, H. (2006). Different Ways to Authenticate Users with the Pros and Cons of each Method. Norweign Computer Center. Retrieved from http://publications.nr.no/directdownload/directdownload/publications.nr.no/rask/old/Authentication_atFHI.pdf
- Adams, A., & Sasse, M. (2003). Users Are Not the Enemy. *Communications of the ACM*, 46(12), 40–46.
- Ajzen, I., & Fishbein, M. (1977). a Theoretical Analysis and Review of Empirical Research. *Psychological Bulletin*, 84(5), 888–918.
<https://doi.org/10.1037/0033-2909.84.5.888>
- Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)* (pp. 248–252).
<https://doi.org/10.1109/ICITST.2014.7038814>
- Amendola, P. J. (2015). *Passwords Made Easy+*. Xlibris Corporation.
- Apple. (2017). Security and your Apple ID. Retrieved March 8, 2016, from <https://support.apple.com/en-za/HT201303>
- Armerding, T. (2017). The 16 biggest data breaches of the 21st century. Retrieved November 8, 2017, from <https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html>
- Baddeley, A. (1997). *Human Memory Theory and Practice* (Illustrate). Psychology Press.
- Bauer, L., Bravo-Lillo, C., Fragkaki, E., & Melicher, W. (2013). A comparison of users' perceptions of and willingness to use Google, Facebook, and Google+ single-sign-on functionality. In *Proceedings of the ACM Conference on Computer and Communications Security* (pp. 25–36).
<https://doi.org/10.1145/2517881.2517886>
- Beaver, K. (2004). Cracking Passwords. In *Hacking for Dummies* (3rd ed., pp. 89–

96). Wiley.

Bonneau, J., Oorschot, P. C. Van, & Stajano, F. (2015). Passwords and the Evolution of Imperfect Authentication. *Communications of the ACM*, 58(7), 78–87. <https://doi.org/10.1145/2699390>

Bonneau, J., & Schechter, S. (2014). Towards Reliable Storage of 56-bit Secrets in Human Memory. In *23rd USENIX Security Symposium (USENIX Security 14)* (pp. 607–623). Retrieved from <https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/bonneau>

Bradford, A. (2017). Deductive Reasoning vs. Inductive Reasoning. Retrieved October 20, 2017, from <https://www.livescience.com/21569-deduction-vs-induction.html>

Bunson, M. (2014). Book of the dead. In *Encyclopedia of Ancient Egypt* (Revised, p. 72). Infobase Publishing.

Butler, R., & Butler, M. . (2015). An Assessment of the Human Factors Affecting the Password Performance of South African Online Consumers (pp. 150–161).

Cameron, D. (2014). Apple warned of iCloud brute-force vulnerability 6 months before Celebgate. Retrieved from <http://www.dailydot.com/debug/apple-icloud-brute-force-attack-march/>

Campbell, J., Ma, W., & Kleeman, D. (2011). Impact of restrictive composition policy on user password practices. *Behaviour & Information Technology*, 30(3), 379–388.

Choong, Y.-Y. (2014). *A Cognitive-Behavioral Framework of User Password Management Lifecycle. Human Aspects of Information Security, Privacy, and Trust*. Springer International. https://doi.org/10.1007/978-3-319-07620-1_12

Choong, Y.-Y., & Theofanos, M. (2015). What 4,500+ People Can Tell You – Employees' Attitudes Toward Organizational Password Policy Do Matter. In *Human Aspects of Information Security, Privacy, and Trust* (pp. 178–189). Springer International. <https://doi.org/10.1007/978-3-319-20376-8>

- Choong, Y.-Y., Theofanos, M., & Liu, H.-K. (2014). United States Federal Employees ' Password Management Behaviors – a Department of Commerce Case Study United States Federal Employees ' Password Management Behaviors – a Department of Commerce Case Study.
- CISO. (2016). NIST Proposes New Approach to Passwords. Retrieved March 15, 2017, from <https://www.cisoadvisory.com/cai-blog/2016/10/24/nist-proposes-new-approach-to-passwords>
- Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The Tangled Web of Password Reuse, (February), 23–26.
- Driscoll, D. (2011). Introduction to Primary Research: Observations, Surveys, and Interviews. *Writing Spaces: Readings on Writing*, 2, 153–174.
- Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human Computer Studies*, 70(6), 415–431. <https://doi.org/10.1016/j.ijhcs.2012.02.008>
- Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., & Herley, C. (2013). Does My Password Go Up to Eleven? The Impact of Password Meters on Password Selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2379–2388). <https://doi.org/10.1145/2470654.2481329>
- Fahl, S., Harbach, M., Acar, Y., & Smith, M. (2013). On the ecological validity of a password study. In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13* (p. 13). ACM. <https://doi.org/10.1145/2501604.2501617>
- Florencio, D., & Herley, C. (2010). Where Do Security Policies Come From ? In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 10).
- Florêncio, D., Herley, C., & Oorschot, P. (2014a). An Administrator's Guide to Internet Password Research. In *Proceedings of the 28th Large Installation System Administration Conference (LISA14)* (pp. 33–52).
- Florêncio, D., Herley, C., & Oorschot, P. Van. (2014b). Password Portfolios and the Finite-Effort User : Sustainably Managing Large Numbers of Accounts. In

23rd USENIX Security Symposium (pp. 575–590).

- Foddy, W. (1994). *Constructing Questions for Interviews and Questionnaires: Theory and Practice in Social Research* (Illustrate). Cambridge University Press.
- Furnell, S. (2007). An assessment of website password practices. *Computers and Security*, 26(7–8), 445–451. <https://doi.org/10.1016/j.cose.2007.09.001>
- Furnell, S., & Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. *Computers and Security*, 31(8), 983–988. <https://doi.org/10.1016/j.cose.2012.08.004>
- Furnell, S., & Thomson, K. L. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. *Computer Fraud and Security*, 2(2), 5–10. [https://doi.org/10.1016/S1361-3723\(09\)70019-3](https://doi.org/10.1016/S1361-3723(09)70019-3)
- Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. *Proceedings of the Second Symposium on Usable Privacy and Security - SOUPS '06*, 44. <https://doi.org/10.1145/1143120.1143127>
- Google. (2017a). Create a strong password. Retrieved November 8, 2017, from <https://support.google.com/accounts/answer/32040?hl=en>
- Google. (2017b). Create your Google Account. Retrieved July 25, 2017, from <https://accounts.google.com/SignUp>
- Guest, G., MacQueen, K., & Namey, E. (2011). *Applied Thematic Analysis* (illustrate). SAGE.
- Haque, S. M. T., Wright, M., & Scielzo, S. (2014). Hierarchy of users' web passwords: Perceptions, practices and susceptibilities. *International Journal of Human Computer Studies*, 72(12), 860–874. <https://doi.org/10.1016/j.ijhcs.2014.07.007>
- Helkala, K. (2011). Password education based on guidelines tailored to different password categories. *Journal of Computers*, 6(5), 969–975.
- Helkala, K., & Hoddø Bakås, T. (2014). Extended results of Norwegian password security survey. *Information Management & Computer Security*, 22(4), 346–

357. <https://doi.org/10.1108/IMCS-10-2013-0079>

Herley, C., & Van Oorschot, P. C. (2012). A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy*, 10(1), 28–36. Retrieved from <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/Persistence-authorcopy.pdf>

Imperva. (2010). Consumer Password Worst Practices. Retrieved May 18, 2017, from https://www.imperva.com/docs/gated/WP_Consumer_Password_Worst_Practices.pdf

Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10* (p. 383). <https://doi.org/10.1145/1753326.1753384>

ISO/IEC 27000. (2012). *Information technology- Security techniques- Information security management systems-Overview and vocabulary*.

ISO/IEC 27002. (2013). *Information technology — Security techniques — Code of practice for information security management*.

Killmeyer, J. (2006). *Information Security Architecture: An Integrated approach to security in the organization* (2nd Editio). New York: Auerbach.

Kraus.SJ. (1995). Attitudes and the prediction of behavior: a meta-analysis of the empirical literature. *Personality and Social Psychology Bulletin*, 21(1), 58–75.

Krippendorff, K. (2012). *Content Analysis: An Introduction to Its Methodology* (Third). SAGE.

Lamont, T. (2016). Life after the Ashley Madison affair. Retrieved March 9, 2017, from <https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked>

Leal, R. (2017). How two-factor authentication enables compliance with ISO27001 access controls. Retrieved March 28, 2017, from <https://advisera.com/27001academy/blog/2017/01/16/how-two-factor-authentication-enables-compliance-with-iso-27001-access-controls/>

- Li, Z., He, W., Akhawe, D., & Song, D. (2014). The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. In *23rd USENIX Security Symposium (USENIX Security 14)*.
- Malone, D., & Maher, K. (2011). Investigating the Distribution of Password Choices. In *Proceedings of the 21st international conference on World Wide Web* (pp. 301–310). <https://doi.org/10.1145/2187836.2187878>
- McCumber, J. (2004). *Assessing and Managing Security Risk in IT systems* (Illustrate). Auerbach.
- McDowell, M., Hernan, S., & Rafail, J. (2009). Security Tip(ST04-002): Choosing and Protecting Passwords. Retrieved from <https://www.us-cert.gov/ncas/tips/ST04-002>
- Microsoft. (2017a). Configuring Password Policies. Retrieved May 2, 2017, from <https://technet.microsoft.com/en-us/library/dd277399.aspx>
- Microsoft. (2017b). Create account. Retrieved July 26, 2017, from https://signup.live.com/?wa=wsignin1.0&rpsnv=13&ct=1509908898&rver=6.7.6643.0&wp=MBI_SSL&wreply=https%253A%252F%252Faccount.microsoft.com%252Fauth%252Fcomplete-signin%253Fru%253Dhttps%25253a%25252f%25252faccount.microsoft.com%25252f%25253frefd%25253daccount.microsoft.com%252526refp%25
- Microsoft. (2017c). Password Policy. Retrieved September 11, 2017, from <https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/password-policy>
- Morris, R., & Thompson, K. (1979). Password security: A case history. *Communications of the ACM*, 22(11), 594–597. <https://doi.org/10.1145/359168.359172>
- NIST SP 800-100. (2006). *Information Security Handbook : A Guide for Managers*. <https://doi.org/10.6028/NIST.SP.800-100>
- NIST SP 800-118. (2009). *Draft NIST Special Publication (SP) 800-118, Guide to Enterprise Password Management (Retired)*. NIST. Retrieved from <http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf>

- NIST SP 800-12. (1995). *An Introduction to Computer Security: The NIST Handbook*.
- NIST SP 800-63-1. (2013). *Electronic Authentication Guideline. NIST Special Publication (Vol. 800)*. <https://doi.org/10.6028/NIST.SP.800-63-2>
- NIST SP 800-63-2. (2013). *Electronic Authentication Guideline (Special Publication 800-63-2)*. Retrieved from <http://dx.doi.org/10.6028/NIST.SP.800-63-2>
- NIST SP 800-63B. (2016). *DRAFT NIST Special Publication 800-63B Digital Identity Guidelines. National Institute of Standards and Technology*. Retrieved from <https://csrc.nist.gov/csrc/media/publications/sp/800-63/3/draft/documents/sp800-63b-draft.pdf>
- NIST SP 800-63B. (2017). *Digital identity guidelines: authentication and lifecycle management*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-63b>
- Olivier, M. (2009). *Information Technology Research (Third)*. Pretario: Van Schaik Publishers.
- Pathak, A. (2013). Graphical password authentication. Retrieved September 7, 2016, from <http://www.slideshare.net/asimkumarpathak/graphical-pswr-d-auth>
- Peltier, T. (2013). *Information Security Fundamentals (second)*. CRC Press.
- Rastogi, V., & Agrawal, A. (2015). All your Google and Facebook logins are belong to us: A case for single sign-off. In *2015 8th International Conference on Contemporary Computing, IC3 2015* (pp. 416–421).
- Renaud, K., Mayer, P., Volkamer, M., & Maguire, J. (2013). Are Graphical Authentication Mechanisms As Strong As Passwords ? In *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems* (pp. 837–844).
- Rouse, M. (2014). Graphical password or graphical user authentication (GUA). Retrieved March 30, 2017, from <http://searchsecurity.techtarget.com/definition/graphical-password>

- Rouse, M. (2015). Single-Factor authentication. Retrieved March 29, 2017, from <http://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA>
- Rouse, M. (2016). Single Sign-On (SSO). Retrieved April 18, 2017, from <http://searchsecurity.techtarget.com/definition/single-sign-on>
- SANS. (2014a). *Password Construction Guidelines*. SANS.
- SANS. (2014b). *Password Protection Policy*. SANS. Retrieved from <https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy>
- Sasse, M., Brostoff, S., & Weirich, D. (2001). Transforming the “Weakest Link”: A Human-Computer Interaction Approach for Usable and Effective Security. *BT Technology Journal*, 19(3), 122–131.
- Sasse, M., Steves, M., Krol, K., & Chisnell, D. (2014). The great authentication fatigue - And how to overcome it. In *6th International Conference, CCD 2014* (Vol. 8528 LNCS, pp. 228–239). https://doi.org/10.1007/978-3-319-07308-8_23
- Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods For Business Students* (6th ed.). Pearson Higher Ed.
- Schneier, B. (2015). Stealing Fingerprints. Retrieved from https://www.schneier.com/blog/archives/2015/10/stealing_finger.html
- Semin, G., & Fiedler, K. (1996). *Applied Social Psychology*. London: SAGE.
- Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., ... Cranor, L. F. (2010). Encountering Stronger Password Requirements : User Attitudes and Behaviors Categories and Subject Descriptors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS '10* (p. 1). <https://doi.org/10.1145/1837110.1837113>
- Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers and Security*, 61, 130–141. <https://doi.org/10.1016/j.cose.2016.05.007>

- Siciliano, R. (2016). Weak Passwords Mean Data Breaches. Retrieved March 3, 2016, from <https://roboform-blog.siber.com/2016/01/08/weak-passwords-mean-data-breaches/>
- Simon, S., & Perkins, R. (2016). Analysis of Data Breach Induced Trauma : An Exploratory Study. *Journal Of Information System Security*, 12(3).
- Sincero, S. (2012). Types of Surveys. Retrieved October 24, 2017, from <https://explorable.com/types-of-survey>
- Skowronek, D., & Duerr, L. (2009). The convenience of nonprobability: Survey strategies for small academic libraries. *College & Research Libraries News*, 70(7), 412–415. <https://doi.org/10.5860/crln.70.7.8221>
- Stobert, E., & Biddle, R. (2014). The Password Life Cycle: User Behaviour in Managing Passwords. In *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS'14)* (pp. 243–255).
- Stobert, E., & Biddle, R. (2015). Expert Password Management. In *Technology and Practice Of Passwords* (pp. 3–20). Retrieved from <https://passwordscon.org/wp-content/uploads/2015/05/preproceedings.pdf>
- Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2011). What makes users refuse web single sign-on?: an empirical investigation of OpenID. In *SOUPS '11: Proceedings of the Seventh Symposium on Usable Privacy and Security* (pp. 1–20).
- Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour and Information Technology*, 29(3), 223–224.
- Taneski, V., Hericko, M., & Brumen, B. (2014). Password security—No change in 35 years? *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on*, (May), 1360–1365.
- Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & 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 - CHI '16*

(pp. 3748–3760). <https://doi.org/10.1145/2858036.2858546>

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., ... Cranor, L. F. (2015). “ I Added ‘!’ at the End to Make It Secure ”: Observing Password Creation in the Lab. In *Proceedings of the eleventh Symposium On Usable Privacy and Security* (pp. 123–140).

Van Eemeren, F., & Grootendorst, R. (2004). *A Systematic Theory of Argumentation*. Cambridge: University of Cambridge.

Verizon. (2015). 2015 Data Breach Investigation Report. Retrieved November 20, 2016, from <http://www.verizonenterprise.com/verizon-insights-lab/dbir/>

Von Solms, S., & Von Solms, R. (2009). *Information Security Governance* (Illustrate). Springer US.

Von Zezschwitz, E., De Luca, A., & Hussmann, H. (2013). Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (pp. 460–467). https://doi.org/10.1007/978-3-642-40477-1_28

Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. (Belin), Cook, J., & Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human Computer Studies*, 65(8), 744–757. <https://doi.org/10.1016/j.ijhcs.2007.03.007>

Walden, D., & Van Vleck, T. (1973). *Compatible Time-Sharing System (1961-1973) Fiftieth Anniversary Commemorative Overview. System*.

Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding Password Choices : How Frequently Entered Passwords Are Re-used across Websites. In *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (pp. 175–188). Retrieved from <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/wash>

Weir, M., Aggarwal, S., Collins, M., & 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 (CCS)* (pp. 162–175).

<https://doi.org/10.1145/1866307.1866327>

Zhang-Kennedy, L., Chiasson, S., & Oorschot, P. Van. (2016). Revisiting Password Rules : Facilitating Human Management of Passwords. In *APWG Symposium on Electronic Research(eCrime)* (pp. 1–10). Toronto, ON: IEEE. <https://doi.org/10.1109/ECRIME.2016.7487945>

Zhang, Y., Monroe, F., & Reiter, M. (2010). The security of modern password expiration-An algorithmic framework and empirical analysis. In *Proceedings of the 17th ACM conference on Computer and communications security* (p. 176). <https://doi.org/10.1145/1866307.1866328>

Zhao, R., & Yue, C. (2014). Toward a secure and usable cloud-based password manager for web browsers. *Computers and Security*, 46, 32–47. <https://doi.org/10.1016/j.cose.2014.07.003>

Appendix A1: Questionnaire

Users' attitude and behaviour towards password policies

Thank you for taking the time out of your busy schedule to complete the survey. The purpose of this survey is to determine users' perceptions towards password policies. Before reading any further please open the password policy by clicking the blue "Click Here" text [Click here](#)

It will take approximately 10-20 minutes to complete the questionnaire. Your participation in this study is completely voluntary. Your survey responses will be strictly confidential and data from this research will be reported only in the aggregate. Your information will be not coded and will remain confidential.

If you have questions at any time about the survey or the procedures, you may contact me Damian Fredericks at s212212435@nmmu.ac.za. Please start with the survey now by clicking on the **Continue** button below.

Section 1: Demographics

1.1 What is your gender?

- Male
- Female

1.2 What is your age group?

- 25 years and under
- 26 to 35 years
- 36 to 55 years
- 56 years and over

1.3 Which of the following best describes you?

- Scholar
- Student
- Employee
- Pensioner

Section 2: Sample Password Policy

The following questions below relate to the sample password policy referred to ([Url link](#))

2.1 How do you feel about the prescribed password minimum length being 8 characters (Section 4.1.1)?

- Very satisfied
- Slightly satisfied
- Neutral
- Slightly dissatisfied
- Very dissatisfied

2.2 How do you feel about the prescribed password maximum length being 16 characters (Section 4.1.1)?

- Very satisfied
- Slightly satisfied
- Neutral
- Slightly dissatisfied
- Very dissatisfied

2.2.a Based on your answer from Question 2.2, why do you feel this way?

2.3 How would you feel if passwords maximum prescribed length was increased to 64 characters?

- Very satisfied
- Slightly satisfied
- Neutral
- Slightly dissatisfied
- Very dissatisfied

2.3.a Based on your answer from Question 2.3, why do you feel this way?

2.4 Do you feel that passwords should have composition requirements as outlined in Section 4.1.3?

- Strongly Agree
- Agree
- Undecided/Neutral
- Disagree
- Strongly disagree

2.5. Would you like the option of using spaces and emoji's (smiley face 😊,sad face ☹) in your passwords?

- Yes
- No
- Undecided

2.6. How often would you prefer to change your passwords?

- Every 60 days
- Every 90 days
- Every 120 days
- Never

2.7 To what extent do you agree or disagree that the general password recommendations are helpful in Section 4.3?

- Strongly Agree
- Agree
- Undecided/Neutral
- Disagree
- Strongly disagree

2.8. Would you like the option to have your newly created passwords automatically checked by the system against a list of commonly compromised passwords before committing to it?

- Yes
- No
- Undecided

2.8.a Based on your answer from Question 2.8, why do you feel this way?

2.9 Would you find the sample password policy difficult to adhere to?

- Yes
- No
- Undecided

2.9.a If answered “Yes” ,what section(s) makes the password policy difficult to adhere to?
Please choose all that apply

- Password Generation
- Password Maintenance
- General Password Recommendations

2.9.b Based on your answer from Question 2.9.a, why would you find the section(s) difficult to adhere to?

Section 3: Behaviour and Coping Strategies

3.1. How often do you use the same password for different accounts?

- Always
- Often
- Sometimes
- Seldom
- Never

3.1 a If you answered Always, Often or Sometimes, why do you use the same password for different accounts? Please choose all that apply

- Find it difficult to come up with a new password
- Do not want to remember multiple passwords
- Find it difficult to remember multiple passwords
- Easier to remember only one password
- Other

3.2 What strategies do you use to create passwords? Please choose all that apply

- Make minor change(s) to an existing password (e.g. %stevie1,#stevie2)
- Use a common name, word or phrase (e.g. how you doing12?)
- Use meaningful mnemonic (e.g. 2beOrnOt@toBee from “to be or not to be”)
- Use random combination of words , letters or characters
- Use character repetitions (e.g. !!!!AAAbbbb9999)
- Use existing passwords from other accounts

- Use password managers (e.g. Lastpass, Roboform)
- Use Single Sign-On (e.g. Facebook login, Google login)

3.3. When constructing a password, which characters do you feel should be included?
Please choose all that apply

- Lowercase
- Uppercase
- Numbers
- Special Characters
- Emoji's
- Spaces

3.4. How do you keep track of your passwords? Please choose all that apply

- Memorize the passwords
- Use "forgot password" feature
- Let browser automatically fill the password in
- Rely on hints provided by system
- Save in a document/file protected with encryption or password
- Save in a document/file not protected(i.e. no encryption or password)
- Share with friend or colleague
- Store in unencrypted electronic devices (e.g. Flash drives, PDA, cellphones)
- Use mnemonics (e.g. meaningful phrases)
- Use password management software (e.g Lastpass, Roboform)
- Write down on paper, but disguise the passwords in some way(e.g. only write down the common word without special characters)
- Write entire password down on paper and store securely in a secure location
- Write entire password down on paper and place in a non- locked location
- Use Single Sign-On (e.g Facebook login, Google login)

3.5. Which of the following coping strategies do you usually adopt? Please choose all that apply

- Reuse my passwords
- Share my passwords
- Write down my passwords on paper
- Save passwords in a document (electronic)
- Use a password manager (e.g. Lastpass, Roboform)
- Use Single Sign-On (e.g. Facebook Login and Google Login)
- Create weak passwords
- Other

3.6 Which of the following Single Sign-On options do you use? Please choose all that apply

- Facebook Login
- Twitter Login
- Google Login
- Microsoft Login

- Apple Login
- LinkedIn account
- Other

3.7 Have you been part of any awareness or educational programs with regard to passwords?

- Yes
- No

3.7.a. Where have you attended the educational or received awareness programs on passwords?.

- School
- University
- Work
- On my own
- Other

Appendix A2: Sample Password Policy

Company XYZ Password Policy

1. Overview

Passwords are the front line of protection for user accounts. A poorly chosen password may result in a compromise of a company's entire network. All employees must adhere to the password policy directives as defined below in order to protect both company and personal information.

2. Purpose

The purpose of this policy is to establish a standard for creating strong passwords, the determining frequency of password change and the protection of those passwords.

3. Scope

The scope of this policy applies to all employees who have an account requiring a password to log into any of Company XYZ systems.

4. Policy

The policy consists of the following sections: Password Generation, Password Maintenance and General Recommendations

4.1 Password Generation

Passwords must meet the following requirements listed below. To prevent passwords from being cracked, passwords should contain a wide range of characters to increase security.

4.1.1. Passwords must be a minimum of 8 characters and a maximum of 16 characters in length.

4.1.2. Passwords must not be solely a dictionary word or a common name.

4.1.3 Passwords must contain at least 3 of the following 4 types of characters:

- Lowercase letters (i.e. a-z)
- Upper case letters (i.e. A-Z)
- Numbers (i.e. 0-9)
- Special characters (e.g. @!#\$%^&*()?)

4.1.4. Passwords must not be the same as the User ID

4.1.5. Users must not reuse previous passwords.

4.1.6. Users must not use the same password for multiple accounts.

4.1.7. Users must not use common acronyms as part of their passwords.

4.1.8. Users must not use names of people or places as part of their passwords.

4.1.9. Users must make their passwords difficult to guess but easy to remember.

4.2 Password Maintenance

Password change is important as it reduces the risk of hackers having access to your accounts.

4.2.1 Minimum password age : Users can keep their passwords for a minimum of 24 hours before being permitted to change it.

4.2.2 Maximum password age : Users can keep their passwords for a maximum of 90 days before being forced to change it.

4.2.3 If your password has been compromised, change it immediately and report it to the helpdesk.

4.3. General Password Recommendations

Further general passwords recommendations listed below can be used to increase the security of passwords.

4.3.1. Do not share your passwords with anyone: family, friends, colleagues, strangers, superiors, etc.

4.3.2. All passwords are to be treated as sensitive and confidential.

4.3.3. Do not write passwords down.

4.3.4. Never send passwords through email.

4.3.5 Never reveal your password over the phone.

4.3.6. Do not use the “Remember Password” feature of applications.

4.3.7. Do not store passwords in a file on any computer system unencrypted.

4.3.8. Ensure you do not allow someone to see you type in your password (shoulder surfing).

4.3.9. Ensure that you delete an account if you are no longer using it.

Disclaimer

This sample password policy was developed from various sources such as SANS institute (SANS,2014), ISO 27002 (ISO/IEC 27002,2013), NIST 800-118 standard. Password policy templates were also used as samples.

Appendix B: Raw Data

Appendix B presents the raw data of the student/scholar and employee groups which was used in Chapter 6, Section 6.5 in order to determine the comparison between the two groups.

Section 2: Sample Password Policy

2.1 How do you feel about the prescribed password minimum length being 8 characters ?			
Likert Scale options	Group	Number Responses	Percentages Responses
Very satisfied	Employee	16	34.8%
	Student/Scholar	9	31.0%
Slightly satisfied	Employee	8	17.4%
	Student/Scholar	8	27.6%
Neutral	Employee	15	32.6%
	Student/Scholar	9	31.0%
Slightly dissatisfied	Employee	6	13.0%
	Student/Scholar	3	10.3%
Very dissatisfied	Employee	1	2.2%
	Student/Scholar	0	0.0%

Question 2.1: Employee Group n=46 and Student/scholar Group n=29

2.2 How do you feel about the prescribed password maximum length being 16 characters?			
Likert Scale Options	Group	Number Responses	Percentages Responses
Very satisfied	Employee	12	26.1%
	Student/Scholar	6	20.7%
Slightly satisfied	Employee	5	10.9%
	Student/Scholar	2	6.9%
Neutral	Employee	9	19.6%
	Student/Scholar	10	34.5%
Slightly dissatisfied	Employee	13	28.3%
	Student/Scholar	5	17.2%
Very dissatisfied	Employee	7	15.2%
	Student/Scholar	6	20.7%

Question 2.2: Employee Group n=46 and Student/Scholar Group n=29

2.3 How would you feel if passwords maximum prescribed length was increased to 64 characters?			
Likert Scale Options	Group	Number Responses	Percentages Responses
Very satisfied	Employee	4	8.7%
	Student/Scholar	7	24.1
Slightly satisfied	Employee	2	4.4%
	Student/Scholar	2	6.9%
Neutral	Employee	9	19.6%
	Student/Scholar	6	20.7%
Slightly dissatisfied	Employee	3	6.5%
	Student/Scholar	2	6.9%
Very dissatisfied	Employee	28	60.8%
	Student/Scholar	12	41.4%

Question 2.3: Employee Group n=46 and Student/Scholar Group n=29

2.4 Do you feel that passwords should have composition requirements as outlined?			
Likert Scale Options	Group	Number Responses	Percentages Responses
Strongly Agree	Employee	18	39.1%
	Student/Scholar	10	35.7%
Agree	Employee	14	30.4%
	Student/Scholar	10	35.7%
Undecided/Neutral	Employee	11	23.9%
	Student/Scholar	7	25.0%
Disagree	Employee	3	6.5%
	Student/Scholar	1	3.6%
Strongly Disagree	Employee	0	0.0%
	Student/Scholar	0	0.0%

Question 2.4: Employee Group n=46 and Student/Scholar Group n=28

2.5 Would you like the option of using spaces and emoji's (smiley face :),sad face :() in your passwords?			
Options	Group	Number Responses	Percentages Responses
Yes	Employee	18	39.1%
	Student/Scholar	13	46.4%
No	Employee	21	45.7%
	Student/Scholar	10	35.7%
Undecided	Employee	7	15.2%
	Student/Scholar	5	17.9%

Question 2.5: Employee Group n=46 and Student/Scholar Group n=28

2.6 How often would you prefer to change your passwords?			
Options	Group	Number Responses	Percentages Responses
Every 60 days	Employee	12	26.1%
	Student/Scholar	3	10.7%
Every 90 days	Employee	8	17.4%
	Student/Scholar	5	17.9%
Every 120 days	Employee	6	13.0%
	Student/Scholar	8	28.6%
Never	Employee	20	43.5%
	Student/Scholar	12	42.8%

Question 2.6: Employee Group n=46 and Student/Scholar Group n=28

2.7 To what extent do you agree or disagree that the general password recommendations are helpful?			
Likert Scale Options	Group	Number Responses	Percentages Responses
Strongly agree	Employee	9	19.6%
	Student/Scholar	10	34.5%
Agree	Employee	28	60.9%
	Student/Scholar	13	44.8%
Undecided	Employee	7	15.2%
	Student/Scholar	5	17.2%
Disagreed	Employee	2	4.3%
	Student/Scholar	1	3.5%
Strongly disagree	Employee	0	0.0%
	Student/Scholar	0	0.0%

Question 2.7: Employee Group n=46 and Student/Scholar Group n=29

2.8 Would you like the option to have your newly created passwords automatically checked by the system against a list of commonly compromised passwords before committing to it?			
Options	Group	Number Responses	Percentages Responses
Yes	Employee	34	73.9%
	Student/Scholar	23	79.3%
No	Employee	7	15.2%
	Student/Scholar	4	13.8%
Undecided	Employee	5	10.9%
	Student/Scholar	2	6.9%

Question 2.8: Employee Group n=46 and Student/Scholar Group n=29

2.9 Would you find the sample password policy difficult to adhere to?			
Options	Group	Number Responses	Percentages Responses
Yes	Employee	5	10.9%
	Student/Scholar	6	20.7%
No	Employee	30	65.2%
	Student/Scholar	21	72.4%
Undecided	Employee	11	23.9%
	Student/Scholar	2	6.9%

Question 2.9: Employee Group n=46 and Student/Scholar Group n=29

2.9a If answered "Yes" What section(s) makes the password policy difficult to adhere to? Please choose all that apply			
Options	Group	Number Responses	Percentages Responses
Password Generation	Employee	2	25.0%
	Student/Scholar	2	25.0%
Password Maintenance	Employee	4	50.0%
	Student/Scholar	4	50.0%
Password Protection	Employee	2	25.0%
	Student/Scholar	2	25.0%

Question 2.9a: Employee Group n=6 and Student/Scholar Group n=6

Section 3: Behaviour and Coping Strategies

3.1 How often do you use the same password for different accounts?			
Options	Group	Number Responses	Percentages Responses
Always	Employee	11	23.9%
	Student/Scholar	8	27.6%
Often	Employee	22	47.8%
	Student/Scholar	14	48.3%
Sometimes	Employee	9	19.6%
	Student/Scholar	6	20.7%
Seldom	Employee	4	8.7%
	Student/Scholar	1	3.4%
Never	Employee	0	0.0%
	Student/Scholar	0	0.0%

Question 3.1: Employee Group n=46 and Student/Scholar Group n=29

3.1a If you answered Always, Often or Sometimes, why do you use the same password for different accounts? Please choose all that apply			
Options	Group	Number Responses	Percentages Responses
Find it difficult to come up with a new password	Employee	11	26.2%
	Student/Scholar	5	17.9%
Do not want to remember multiple passwords	Employee	25	59.5%
	Student/Scholar	19	67.9%
Find it difficult to remember multiple passwords	Employee	24	57.1%
	Student/Scholar	12	42.9%
Easier to remember	Employee	23	54.8%
	Student/Scholar	15	53.6%
Other	Employee	2	4.8%
	Student/Scholar	0	0.0%

Question 3.1a: Employee Group n=42 and Student/Scholar Group n=28

3.2 What strategies do you use to create passwords? Please choose all that			
Options	Group	Number Responses	Percentages Responses
Make minor change(s) to an existing password (e.g. %stevie1,#stevie2)	Employee	30	65.2%
	Student/Scholar	19	65.5%
Use a common name, word or phrase(e.g. how you doing12?)	Employee	12	26.0%
	Student/Scholar	8	27.6%
Use meaningful mnemonic (e.g 2beOrnOt@toBee from "to be or not to be")	Employee	13	28.2%
	Student/Scholar	6	20.7%
Use random combination of words , letters or characters	Employee	14	30.4%
	Student/Scholar	8	27.6%
Use character repetitions (e.g !!!!AAAbbbb9999)	Employee	2	4.3%
	Student/Scholar	2	6.9%
Use existing passwords from other accounts	Employee	18	39.1%
	Student/Scholar	17	58.6%
Use password managers (e.g Lastpass, Roboform)	Employee	1	2.2%
	Student/Scholar	1	3.4%
Use Single Sign-on (e.g. Facebook login, Google login)	Employee	13	28.3%
	Student/Scholar	6	20.7%

Question 3.2: Employee Group n=46 and Student/Scholar Group n=29

3.3 When constructing a password, which characters do you feel should be included? Please choose all that apply			
Options	Group	Number Responses	Percentages Responses
Lowercase	Employee	34	73.9%
	Student/Scholar	21	72.4%
Uppercase	Employee	39	84.8%
	Student/Scholar	23	79.3%
Numbers	Employee	39	84.8%
	Student/Scholar	25	86.2%
Special Character	Employee	34	73.9%
	Student/Scholar	18	62.1%
Emoji's	Employee	11	23.9%
	Student/Scholar	3	10.3%
Spaces	Employee	3	6.5%
	Student/Scholar	7	24.1%

Question 3.3: Employee Group n=46 and Student/Scholar Group n=29

3.4 How do you keep track of your passwords?			
Options	Group	Number Responses	Percentage Responses
Memorise the password	Employee	34	73.9%
	Student	27	93.1%
Use Single Sign-On	Employee	17	36.9%
	Student	9	31.0%
Use "forget password" feature	Employee	18	39.1%
	Student	11	37.9%
Let browser autofill	Employee	7	15.2%
	Student	10	34.5%
Rely on hints provided by systems	Employee	7	15.2%
	Student	3	10.3%
Save in a document/file protected with encryption	Employee	8	17.4%
	Student	2	6.9%
Save in a document/file not protected	Employee	2	4.3%
	Student	0	0.0%
Share with friend or colleague	Employee	0	0.0%
	Student	0	0.0%
Store in encrypted electronic devices	Employee	5	10.9%
	Student	1	3.4%
Use mnemonics	Employee	3	6.5%
	Student	5	17.2%
Use password management software	Employee	5	10.9%
	Student	0	0.0%
Write down on paper but disguise in some way	Employee	12	26.1%
	Student	4	13.8%
Write entire password down on paper and store securely in a locked location	Employee	5	10.9%
	Student	2	6.9%
Write entire password down on paper and place in a non-locked location	Employee	2	4.3%
	Student	0	0.0%

Question 3.4: Employee Group n=46 and Student/Scholar Group n=29

3.5 Which of the following coping strategies do you usually adopt? Please choose all that apply			
Options	Group	Number Responses	Percentages Responses
Reuse my passwords for multiple accounts	Employee	39	84.8%
	Student/Scholar	26	89.7%
Share my passwords with others	Employee	0	0%
	Student/Scholar	1	3.4%
Write down my passwords on paper	Employee	11	23.9%
	Student/Scholar	4	13.7%
Write down my passwords in a document	Employee	5	10.9%
	Student/Scholar	3	10.3%
Use a password manager (e.g Lastpass, Roboform)	Employee	6	13.0%
	Student/Scholar	0	0.0%
Use Single Sign On (e.g Facebook login, Google login)	Employee	14	30.4%
	Student/Scholar	7	24.1%
Create weak passwords	Employee	4	8.7%
	Student/Scholar	1	3.4%

Do not change my passwords unless forced to change it	Employee	28	60.9%
	Student/Scholar	18	62.1%
Other	Employee	1	2.2%
	Student/Scholar	1	3.4%

Question 3.5: Employee Group n=46 and Student/Scholar Group n=29

3.6 Which of the following Single Sign On do you use? Please choose all that			
Options	Group	Number Responses	Percentages Responses
Facebook Login	Employee	34	73.9%
	Student/Scholar	19	65.5%
Twitter Login	Employee	5	10.9%
	Student/Scholar	2	6.9%
Google Login	Employee	23	50.0%
	Student/Scholar	20	68.9%
Microsoft Login	Employee	8	17.4%
	Student/Scholar	5	17.2%
Apple Login	Employee	8	17.4%
	Student/Scholar	2	6.9%
LinkedIn account	Employee	10	21.7%
	Student/Scholar	4	13.8%
None	Employee	8	17.4%
	Student/Scholar	5	17.2%
Other	Employee	2	4.3%
	Student/Scholar	1	3.4%

Question 3.6: Employee Group n=46 and Student/Scholar Group n=29

3.7 Have you been part of any awareness or educational programs with regard to passwords?			
Options	Group	Number Responses	Percentages Responses
Yes	Employee	10	21.8%
	Student/Scholar	10	34.5%
No	Employee	36	78.2%
	Student/Scholar	19	65.5%

Question 3.7: Employee Group n=46 and Student/Scholar Group n=29

3.7a Where have you attended the educational or received awareness programs on passwords?			
Options	Group	Number Responses	Percentages Responses
School	Employee	2	20.0%
	Student/Scholar	1	10.0%
University	Employee	7	70.0%
	Student/Scholar	10	100.0%
Work	Employee	8	80.0%
	Student/Scholar	0	0.0%
On my own (website, YouTube, videos)	Employee	3	30.0%
	Student/Scholar	1	10.0%
Other	Employee	0	0.0%
	Student/Scholar	0	0.0%

Question 3.7a: Employee Group n=10 and Student/Scholar Group n=10

Appendix C: HAISA Paper

Comparing student password knowledge and behaviour: A case study

D.T. Fredericks¹, L.A. Futcher² and K.Thomson³

Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University
Port Elizabeth, South Africa

¹+27 833793400
s212212435@nmmu.ac.za x

²+27 41 504 9128

Lynn.futcher@nmmu.ac.za

³+27 41 504 3048

Kerry-lynn.thomson@nmmu.ac.za

Abstract:

Passwords have been around for a long time, but today more than ever, users have to remember many passwords for different accounts. As a result, users tend to create simple passwords to access their accounts. When users create simple passwords they do not realise the possible repercussions that may arise. Statistics show that many data breaches have happened over the years because of poor password management. This paper discusses the importance of good password management. Passwords go through a lifecycle including creation, storage, maintenance and deletion. At each phase of the lifecycle, users should understand what is required to ensure good password management. In addition, this paper provides the results of a survey carried out at a university in South Africa. The survey took the form of a questionnaire and was distributed to Information Technology students ranging from 1st to 4th year. The aim of the survey was to determine student knowledge and their behaviour with regards to password management. The results and findings from the survey indicated that the respondents are educated with regards to good password management. However, it was discovered that not all users are putting that knowledge into practice, which highlights a significant vulnerability regarding their password behaviour.

Keywords:

Password management, password knowledge, password behaviour

1. Introduction

Passwords play an important role in everyday lives. They are used to log into personal computers, email accounts, bank accounts and company computers. Passwords act as a protective barrier between the user and their personal information (McDowell *et al*, 2013). Therefore, users should choose strong, secure passwords to protect their personal information from attackers. Many people, however, are still generating weak passwords and exhibiting bad practices, such as writing their passwords down or using the same password for multiple accounts (Renaud *et al*, 2013). Having weak passwords also puts bank accounts, and other information, at risk of being hacked (Blanchard, 2014). Often when users generate their passwords they have a guessable structure behind them. An example would be passwords that just have words or numbers for passwords and no combination of alphanumeric characters (Helkala, 2011). To further emphasise that users generate weak passwords, Splashdata released its annual list of the 25 most common passwords found amongst users. In this report, the *top three* most common passwords were “123456”, “password” and “12345678”. Based on the report, a further finding was that most of the passwords were “word” passwords and numeric passwords, making them easier to guess. This could put user and company information at risk (TeamsID, 2016).

This paper discusses password management, firstly, by detailing related work in Section 2, and then discussing the importance of good password management in Section 3. Section 4 describes the design of the questionnaire while Section 5 presents the survey results and findings which are further discussed in Section 6. Finally, the paper is concluded in Section 7.

2. Related work

A number of related surveys have been conducted with regard to passwords. Gaw and Felten (2006) conducted a survey with 49 undergraduate respondents where the respondents were asked how many passwords they had and how often they reuse their passwords. From this survey, it was determined that users have a high number of reused passwords and that users rely heavily on memory and password reminder features to remember their passwords. From the results, it was determined that as respondents progress through their year of studies, they use more online accounts and they would reuse passwords more often (Gaw & Felten, 2006).

Additional studies have been done, measuring password strength against password cracking algorithms (Kelley *et al*, 2012) and testing metrics for password creation policies (Weir *et al*, 2010). However, while extensive studies have been conducted on passwords, there has been limited research done regarding the gap between the knowledge and behaviour of users with regards to password management.

3. Importance of good password management

In order to protect their personal and organizational information, users need to know the importance of good password management. According to Stobert and Biddle passwords go through a cycle of four phases (Stobert and Biddle, 2014) including: Creation, Storage, Maintenance and Deletion as discussed in the following subsections.

3.1 Creation Phase

Having a strong password provides a line of defence against unauthorised access to one's computer and personal information. The stronger the password, the lower the chances of users getting hacked and being exposed to malicious software (Microsoft, 2015). According to various sources (Microsoft, 2015; Apple, 2013; Google, 2016) strong passwords should adhere to various criteria relating to password length and content. For example, a combination of letters, numbers and symbols. In addition to the recommended criteria, various other tips are available to help users create strong passwords.

3.2 Storage Phase

According to the University of Illinois (2014) "*using the same password for all of your accounts is like having one key that unlocks every door in your life*". If users use the same password for multiple accounts, it would not take long for a smart hacker to identify which sites they can use these hacked passwords on. Users can make use of password managers to store passwords if they have many passwords that they utilize. A password manager is a database which stores users' passwords and usernames for different sites (Li *et al*, 2014). However, Chiasson *et al* mention that password managers have drawbacks as they typically use a master password for all user accounts. If the attacker gains access to the master password, then the attacker would gain full control over the user accounts (Chiasson *et al*, 2009). Renaud *et al* (2013) state that "*password managers are no substitution for a secure and usable authentication*". Password managers can be used, but users must understand that there are risks involved. Examples of password managers include LastPass, RoboForm, Mylogin and PasswordBox.

3.3 Maintenance Phase

Microsoft's password policy states that a best practice on the maximum password age should be between 30 and 90 days depending on the environment. By changing a password, an attacker has a limited amount of time in which they can compromise a user's password (Microsoft, 2012). According to Apple (2016), users should change their passwords regularly and avoid reusing passwords. One of the characteristics of strong passwords is that people should create passwords different from previously used passwords. If users want to update their passwords, they should create a brand new password.

3.4 Deletion Phase

Stobert and Biddle (2014) mention that users tend to forget passwords because of lack of memorability. If a user is no longer using an online account, it should be decided whether to keep it or delete it. There are risks involved if users decide to keep their accounts even though they are not using that specific online account. Such accounts can be compromised by hackers even though they do not use that account anymore because their personal information is stored (Schofield, 2013). To avoid this from happening, users should delete accounts if they have not used their accounts for a considerable period of time.

4. Questionnaire design

The aim of the survey was to determine the students' theoretical knowledge with regard to good password management compared to their actual password behaviour. The survey was divided into 3 sections: Section 1 addressed the demographics, Section 2 focused on the theoretical password knowledge and Section 3 addressed the actual password behaviour of the respondents. Each section had multiple questions. Most questions were closed questions with restricted options available. These options are indicated in brackets in Tables 1 and 2.

Section 1: Demographics: This section required the respondents to indicate their current year of study.

Section 2: Theoretical password knowledge: The purpose of this section was to determine the respondents' theoretical knowledge relating to good password management.

Q	Question description
Q2.1	Have you received guidance on password creation in the past? (Yes, No)
Q2.2	If 'Yes' Where or from Whom? (While studying, Websites/Newspaper, From friends or Other)
Q2.3	In your opinion, what should be the minimum character length of a password? (6, 7, 8, 9, 10)
Q2.4	In your opinion, a password should consist of (Uppercase letters, Lowercase Letters, Combination of both)
Q2.5	In your opinion, should a password contain symbols e.g @,!,\$,<,#,? (Yes, No, Don't know)
Q2.6	How often should users change their password? (Every 90 days, Every 120 days, Never, Don't know)
Q2.7	Should users delete their online accounts if they are not using them? (Yes, No, Don't know)
Q2.8	Should users write down their passwords on notes, in text files, etc.? (Yes, No, Don't know)
Q2.9	Briefly, describe what a good password should contain. (Open ended)

Table 1: Theoretical password knowledge questions

The results of these questions are discussed in Section 5.2

Section 3: Actual password behaviour: The purpose of this section was to determine the respondents' actual password behaviour. A Likert scale ranging from 1 to 5 was used for certain questions as shown in Table 2, where 1 = 'always', 3 = 'sometimes' and 5 = 'never'. The results of the Likert scale questions are shown in Table 5.

Q	Question description
Q3.1	Do you reuse your password over a period of time? (1 to 5)
Q3.2	Do your passwords only contain plaintext (no special symbols and alphanumeric characters) (1 to 5)
Q3.3	Are your password lengths less than 10 characters? (1 to 5)
Q3.4	Have you ever used the same password for multiple accounts e.g FaceBook, Gmail, NMMU account? (Yes, No)

Q3.5	Have you ever used `12345` or `password` for a password? (Yes, No)
Q3.6	Have you ever used family member names, usernames and personal dates as passwords? (1 to 5)
Q3.7	Have you ever used dictionary words as passwords? (1 to 5)
Q3.8	How often do you change your passwords? (Every 90 days, Every 120 days, Never, Don't know)
Q3.9	Which of the following statements is best suited to describe how you remember your passwords? (Often remember, Reset if cannot remember, Remember, Other)
Q3.10	Do you write your passwords down? (Yes, No, Sometimes)
Q3.11	If 'Yes' where do you write your passwords down? (In a text file, On a note, Password Manager, Don't know, Other)
Q3.12	Do you share your passwords? (Yes, No)
Q3.13	If 'Yes', who do you share them with? (Family, Friends, Colleagues, Peers)
Q3.14	Do you delete your online accounts if you haven't used them in a long time? (Yes, No)
Q3.15	Do you reuse your regular passwords in the accounts/services that you think should be extra protected? (1 to 5)

Table 2: Actual password management behaviour questions

The results of these questions are discussed in Section 5.3

5. Survey results and findings

This section reports on the results and findings of a survey carried out at a university in South Africa. The respondents consisted of IT students ranging from 1st year to 4th year.

5.1 Demographic results

The survey had a total of 45 respondents. In terms of the year of study, there were 5 (11%) 1st Years, 10 (22%) 2nd Years, 16 (36%) 3rd years and 14 (31%) 4th years.

5.2 Theoretical password knowledge

Tables 3 indicates responses to the (Yes, No) questions in Section 2 of the questionnaire.

Question	Yes	No	Don't know
Q2.1	34	11	0
Q2.5	29	12	4
Q2.7	29	10	6
Q2.8	4	39	2

Table 3: Theoretical options (n=45)

For Q2.1, 34 (75%) respondents stated having received guidance on creating passwords. For Q2.5, 29 (64%) respondents suggested that a password should contain symbols, whereas 12 (26%) respondents said 'No' and 4 (8%) respondents stated that they 'Don't Know'. For Q2.7, 29 (64%) respondents suggested that online accounts should be deleted if not being used. For Q2.8, 39 (86%) respondents stated that passwords should not be written down, whereas 4 (8%) respondents said 'Yes' that users should write down their passwords.

Table 4 below represents theoretical password knowledge questions results. The greyed out options indicated the options the respondents had to choose from.

Question	Option 1	Option 2	Option 3	Option 4	Option 5
Q2.2	While Studying	Websites/ Newspaper	From Friends	Other	
	19	10	1	4	
Q2.3	6	7	8	9	10
	12	1	25	2	5
Q2.4	Lowercase	Uppercase	Combination		
	0	0	45		
Q2.6	Every 90 days	Every 120 days	Never	Don't know	
	38	4	1	2	

Table 4: Theoretical questions results (n=45)

As can be seen in Table 4, Q2.2, 19 (42%) respondents stated they received password guidance whilst studying and 10 (22%) respondents stated receiving password guidance from websites or newspapers. For Q2.3, 25 (55%) respondents indicated that the minimum number of characters is 8, 12 (26%) respondents indicated a minimum of 6 characters. For Q2.4, 100% of the respondents indicated that a password should contain a combination of uppercase and lowercase characters. For Q2.6, 38 (84%) respondents answered that users should change their passwords every 90 days.

For the open-ended question, Q2.9, most of the respondents indicated that a password should contain a combination of uppercase and lowercase characters, numbers and special characters. Based on these results, it is clear that the respondents are equipped with the necessary theoretical knowledge with regard to good password management.

5.3 Actual password behaviour

This section discusses the results and findings relating to the actual password behaviour of students. Table 5 lists the questions which were asked using a 5-point Likert Scale where 1 = 'always', 3 = 'sometimes' and 5 = 'never'. Those questions not using this scale are omitted from this table but are discussed in this section.

In Table 5, the numbers in brackets are calculated as follows – the number of respondents is multiplied by the Likert Scale option number. For example, 11 respondents chose option 2 for Q3.1. Therefore, the number in brackets is $11 \times 2 = 22$. All the numbers in brackets are then added together for the Total. The Average is calculated by dividing the Total by the number of respondents (n=45).

Questions	Scale					Tot	Avg
	1	2	3	4	5		
Q 3.1	13 (13)	11 (22)	11 (33)	7(28)	3 (15)	111	2.47
Q 3.2	4 (4)	4 (8)	7 (21)	7(28)	23 (115)	176	3.91
Q 3.3	12 (12)	10 (20)	10 (30)	4(16)	9 (45)	123	2.73
Q 3.6	4 (4)	5 (10)	8 (24)	5(20)	23 (115)	173	3.84
Q 3.7	1 (1)	3 (6)	5 (15)	3 (12)	33 (165)	199	4.42
Q 3.15	1 (1)	3 (6)	7 (21)	9 (36)	25 (125)	189	4.2

Table 5: Likert scale questions (n=45)

Table 5 depicts the average for the questions which made use of a 5-point Likert Scale. Those questions with an average of 4.0 or higher, indicate good password behaviour, whereas those with an average of less than 3.0 indicate fairly poor behaviour. From this it can be argued that the respondents behave best when it comes to never using dictionary words as passwords and they generally use stronger passwords to protect those accounts which require extra protection.

For Q3.1, 13 (28%) respondents stated they 'always' reuse their password whereas 3 (6%) respondents stated they 'never' reuse their passwords. For Q3.2, 23 (51%) respondents said their passwords were 'never' plaintext only, whereas 4 (8%) respondents' passwords are 'always' plaintext. For Q3.3, 12 (26%) respondents stated that their passwords were 'always' less than 10 characters, 10 (22%) respondents indicated 'sometimes' and a further 10 (22%) stated their passwords are 'sometimes' less than 10 characters. For Q3.6, 23 (51%)

respondents stated that they ‘never’ use personal dates and family member names as passwords. For Q3.7, 33 (73%) respondents said they ‘never’ use dictionary words as passwords, and for Q3.15, 25 (55%) respondents stated that they ‘never’ use their regular password in the accounts they think should be extra protected.

For Q3.4, 40 (89%) respondents have used the same password for multiple accounts. Similarly, for Q3.5, 40 (89%) respondents said ‘No’ to this question. This is a good sign and shows that a large number of people do not use such simple passwords. For Q3.8, 14 (31%) respondents indicated that they change their passwords every 120 days and 7 (16%) participants do not change their passwords at all. For Q3.8, 6 (13%) respondents actually change their passwords every 90 days. For Q3.12, 39 (87%) respondents do not share passwords. For Q3.14, 17 (37%) respondents do not delete their online accounts if they have not used them in a long time.

6. Discussion

This section discusses the results and findings from the survey by comparing the theoretical password knowledge with the actual password behaviour. There are a number of theoretical password knowledge questions, as were seen in Table 1, which can be correlated to the actual password behaviour questions, as seen in Table 2. Table 6 lists the theoretical and behaviour-related questions that can be correlated.

Characteristic	Theoretical Password Knowledge Questions	Actual Password Behaviour Questions
Minimum password length	Q2.3	Q3.3
Password characteristics	Q2.4	Q3.2
Changing passwords	Q2.6	Q3.8
Delete online accounts	Q2.7	Q3.14
Writing passwords down	Q2.8	Q3.10

Table 6: Correlation between theoretical password knowledge and actual password behaviour questions

Figure 1 represents the respondents’ theoretical password knowledge compared to their actual password management behaviour. For these results, only the top most answered questions are represented. For example, Q2.3, 25 (56%) of the respondents indicated that the minimum password length should be 8 characters, whereas in Q3.3 only 9 (20%) of the respondents indicated that their passwords are ‘always’ less than 10 characters.

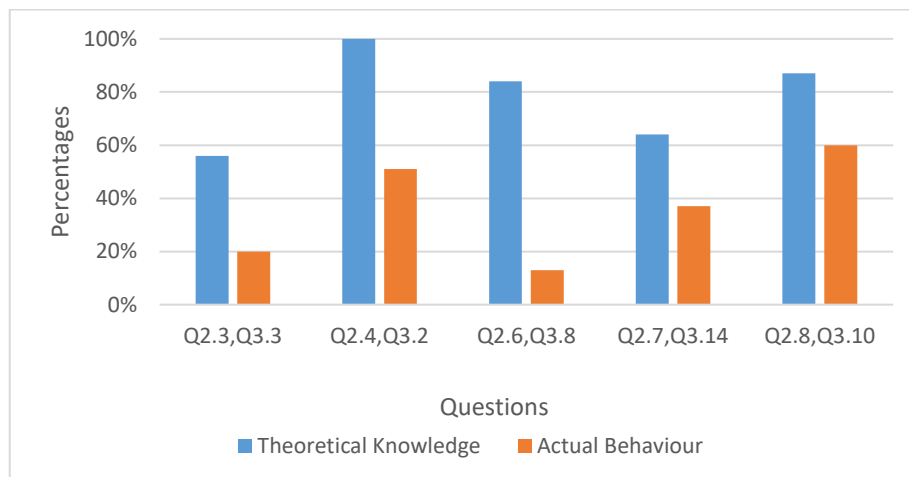


Figure 1: Theoretical knowledge versus actual behaviour

As can be seen in Figure 1, there is a difference between the respondents’ theoretical password knowledge and their actual password behaviour. In Q2.3 and Q3.3, which referred to the minimum password length, it can be seen that the respondents know what the minimum average length should be for a password but when it comes to actually putting it into practice they are not adhering to it. Q2.4 and Q3.2, which referred to the password characteristics, show that the users are aware of the fact that a password should contain a combination of uppercase and lowercase characters. However, when it comes to the actual behaviour, only 23 (51%) of the respondents put the theory into practice by stating they ‘never’ use passwords which are plaintext. In Q2.6 and

Q3.8 which referred to how often passwords should be changed, 38 (84%) of the respondents indicated that they know how often to change their passwords, but do not use this knowledge in practice. In Q2.7 and Q3.14, which referred to the deleting of online accounts, it can be seen that the respondents know that online accounts should be deleted if they are not using it, but are not using this theoretical knowledge in practice. Lastly, Q2.8 and Q3.10, which referred to writing passwords down, show that respondents are aware that they should not write their passwords down, however, with regards to their actual behaviour there is still a large number of people who write passwords down on text files and sticky notes.

7. Conclusion

As discussed, it is very important that people understand the importance of passwords and password management. Based on the theoretical password knowledge results and findings from the survey conducted, it can be seen that these respondents are educated on good password management and have the necessary theoretical knowledge. However, from the actual password behaviour results and findings, it can be seen that there is a difference between the respondents' knowledge and their actual behaviour. By not applying the theoretical password knowledge in practice, it can be argued that users are exposing themselves to risk. This research was limited in that it focused on IT students and the results are not to be generalised. Further research is required to understand this identified gap between users' password knowledge and behaviour. It could be argued that good password behaviour is more likely to be demonstrated by those users who have experienced the consequences of poor password behaviour, thereby re-enforcing the importance of good password management.

8. Acknowledgements

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

References

- Apple (2013). OS X Mountain Lion: Tips for creating secure passwords. Apple.[online] Available at: https://support.apple.com/kb/PH10624?locale=en_US [Accessed 26 April. 2015]
- Apple (2016). Security and your apple ID. Apple.[online] Available at: <https://support.apple.com/en-za/HT201303> [Accessed 8 March.2016]
- Blanchard.J. (2014). Weak passwords put millions at risk of bank accounts and other information being hacked online. Mirror.[online] Available at: <http://www.mirror.co.uk/news/technology-science/technology/weak-passwords-put-millions-risk-4439460> [Accessed 25 March.2015]
- Chiasson, S., Forget, A., Stobert, E., van Oorschot, P.C. and Biddle, R., 2009, November. Multiple password interference in text passwords and click-based graphical passwords. *In Proceedings of the 16th ACM conference on Computer and communications security* (pp. 500-511). ACM.
- Gaw, S. and Felten, E.W., 2006, July. Password management strategies for online accounts. *In Proceedings of the second symposium on Usable privacy and security* (pp. 44-55). ACM.
- Google (2016). Name and password guidelines. Google.[online] Available at: <https://support.google.com/a/answer/33386?hl=en> [Accessed 8 March.2016]
- Helkala, K., 2011. Password education based on guidelines tailored to different password categories. *Journal of Computers*, 6(5), pp.969-975.
- Helkala, K. and Hoddø Bakås, T., 2014. Extended results of Norwegian password security survey. *Information Management & Computer Security*, 22(4), pp.346-357.
- Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F. and Lopez, J., 2012, May. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. *In Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 523-537). IEEE.
- Li, Z., He, W., Akhawe, D. and Song, D., 2014. The emperor's new password manager: Security analysis of web-based password managers. *In 23rd USENIX Security Symposium (USENIX Security 14)* (pp. 465-479).
- McDowell, M., Hernan.S & Rafail.J. (2013). Security Tip(ST04-002): Choosing and Protecting Passwords. US-CERT.[online] Available at: <https://www.us-cert.gov/ncas/tips/ST04-002> [Accessed 25 March. 2015]

Microsoft (2012). Maximum password age. Microsoft.[online] Available at:[https://technet.microsoft.com/en-us/library/hh994573\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/hh994573(v=ws.10).aspx) [Accessed 27 April,2015]

Microsoft.(2015).Tips for creating a strong password. Microsft.[online] Available at: <http://windows.microsoft.com/en-za/windows-vista/tips-for-creating-a-strong-password> [Accessed 25 April,2015]

Renaud, K., Mayer, P., Volkamer, M. and Maguire, J., 2013, September. Are graphical authentication mechanisms as strong as passwords?. *In Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on* (pp. 837-844). IEEE.

Schofield, J. (2013). Hotmail are my lost accounts a security risk.The Guardian.[online] Available at: <http://www.theguardian.com/technology/askjack/2013/jul/18/hotmail-lost-accounts-security-risk> [Accessed 15 June. 2015]

Stobert, E. and Biddle, R., 2014. The password life cycle: user behaviour in managing passwords. *In Symposium On Usable Privacy and Security (SOUPS 2014)* (pp. 243-255).

TeamsID (2016). Worst Passwords Of 2015.[online] Available at: <https://www.teamsid.com/worst-passwords-2015/> [Accessed 10 March. 2016]

University of Illinois (2014). Why you should use different passwords. University of Illinois.[online] Available at: <https://security.illinois.edu/content/why-you-should-use-different-passwords> [Accessed 30 April,2015]

Weir, M., Aggarwal, S., Collins, M. and Stern, H., 2010, October. 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.

Appendix D: Proof Reader Declaration

With reference to the Master's dissertation of Damian Todd Fredericks entitled *Users' Perceptions Regarding Password Policies*,

I, Shekinah Yasmine Kilian, hereby declare that:

- This dissertation was proofread in November 2017.
- The discretion of the author was not abrogated in any way.
- The final version of the dissertation reflects the authorial voice of the student.
- The writing is of a good academic standard.

Shekinah Yasmine Kilian

Bachelor of Arts, University of Port Elizabeth (1990); **Higher Diploma in Education**, University of Port Elizabeth (1994); **Bachelor of Arts Honours**, Vista University (1995); **Master of Philosophy** (Second Language Studies) *cum laude*, Stellenbosch University (2001); **Diploma in Language and Communication** (with specialisation in Forensic Linguistics) *cum laude*, Cardiff University (2005)

yasminekilian@gmail.com