A study of South African computer users' password usage habits and attitude towards password security

Submitted in partial fulfilment
of the requirements of the degree of

Masters of Science

of Rhodes University

Brandon Friendman

Grahamstown, South Africa
May 2014

Abstract

The challenge of having to create and remember a secure password for each user account has become a problem for many computer users and can lead to bad password management practices. Simpler and less secure passwords are often selected and are regularly reused across multiple user accounts. Computer users within corporations and institutions are subject to password policies, policies which require users to create passwords of a specified length and composition and change passwords regularly. These policies often prevent users from reusing previous selected passwords. Security vendors and professionals have sought to improve or even replace password authentication. Technologies such as multi-factor authentication and single sign-on have been developed to complement or even replace password authentication. The objective of the study was to investigate the password habits of South African computer and internet users. The aim was to assess their attitudes toward password security, to determine whether password policies affect the manner in which they manage their passwords and to investigate their exposure to alternate authentication technologies. The results from the online survey demonstrated that password practices of the participants across their professional and personal contexts were generally insecure. Participants often used shorter, simpler and ultimately less secure passwords. Participants would try to memorise all of their passwords or reuse the same password on most of their accounts. Many participants had not received any security awareness training, and additional security technologies (such as multi-factor authentication or password managers) were seldom used or provided to them. The password policies encountered by the participants in their organisations did little towards encouraging the users to apply more secure password practices. Users lack the knowledge and understanding about password security as they had received little or no training pertaining to it.

Acknowledgements

I would like to express my gratitude to my supervisors, Prof. Barry Irwin and John Richter, for providing support and feedback throughout the process of researching and writing of this paper.

I would like to thank all of my family, friends and colleagues for their interest and participation in this study. I would especially like to thank Joon Radley for his time spent helping me with formatting and compiling the LaTeX document.

I would like to thank Emran Mohd Tamil for his permission to use the questions from his research paper in this study.

I am profoundly grateful to my wife and children for their patience, support and love throughout the duration of this research. I would not have made it without them.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Passwords form a significant part of most users' computer experience and online activities. Users are increasingly required to manage a large number of username and password credentials that will allow them to gain access to their personal and corporate resources. An increasingly popular method for dealing with multiple website accounts is the use of a federated login account provided by some of the largest social websites including Google[1], Facebook[2] and Twitter[3]. This facility requires users to only provide the credentials for one of the social websites in order to gain access to the website they are on. There are, however, many websites that do not provide this federated account login and users are still required to maintain a separate set of credentials for those websites.

Consequently, users face the increasingly difficult task of not only trying to remember all of their usernames and passwords (Zhang, Luo, Akkaladevi, and Ziegelmayer, 2009) but they are also (in some cases) required to adhere to a restrictive password policy system within their organisation. Research conducted by Microsoft (Florencio and Herley, 2007) found that users tend to follow bad habits when it comes to password management. For example, they generally tend to use shorter and simpler passwords. They also reuse the same password for multiple user accounts and include personally identifiable information when formulating their passwords (Brown, Bracken, Zoccoli, and Douglas, 2004).

[1] http://code.google.com/apis/accounts/docs/OpenID.html
[2] https://developers.facebook.com/docs/authentication
[3] http://dev.twitter.com/pages/auth

Organisations have incorporated best practice guides on password policies to enforce that their users adhere to a more disciplined and secure approach to password management (Scarfone and Souppaya, 2011). Password security forms an important part of the access control for many organisations and is often implemented in order to achieve compliancy or governance requirements (Williams, 2013) such as Payment Card Industry Data Security Standard[4] (PCI-DSS) and Sarbanes-Oxley[5] (SOX) compliance. Password security, in many cases, is also a significant component of an organisation's security defences; however, even professional information security companies have been exposed and compromised for having failed to implement secure password management practices. This was the case when hacker group 'Anonymous' gained unauthorised access to the servers and Twitter accounts of staff members at HBGary (Wisniewski, 2011).

Organisations are encouraged to educate their users on the these compliancy requirements through the use of security awareness training programmes which provide users with the knowledge and motivation to adhere to the security rules (Bulgurcu, Cavusoglu, and Benbasat, 2010). Users within organisations have demonstrated that security awareness programmes increase their confidence and knowledge about information security (Cooper, 2008) and allow them to integrate security fundamentals into their work ethos.

Users that are exposed to password management best practices and techniques used in enterprise password management should understand the importance of this concept. These users should not only be applying these best practices in their professional or academic capacity but also in their own personal capacity when managing their login credentials for personal websites and private digital resources.

1.2 Statement of the Problem

Research such as "Password security: What users know and what they actually do" (Riley, 2006), "A large-scale study of web password habits" (Florencio and Herley, 2007), "User Behaviours Associated with Password Security and Management" (Bryant and Campbell, 2006) and "Authentication and supervision: A survey of user attitudes" (Furnell, Dowland, Illingworth, and Reynolds, 2000) has identified serious problems regarding password management. These problems include users creating and using insecure passwords that are significantly easy to guess or crack. Additionally, users also employ insecure

[4]https://www.pcisecuritystandards.org
[5]http://www.gpo.gov/fdsys/pkg/PLAW–107publ204/html/PLAW–107publ204.htm

password management practices by reusing passwords on different accounts and storing their passwords in an insecure manner.

Users have difficulty trying to cope with managing a large number of user credentials. This problem, consequently, leads to the frequent use of uncomplicated and short passwords. Furthermore, users tend to reuse the same password across multiple accounts and seldom change the password for their user account.

Criminal and hackers are able to crack and discover users' passwords in a short period of time using commodity computer hardware (Goodin, 2013a). There are numerous password cracking tools available on the internet such as hashcat[6] and John the Ripper[7]. These software tools are freely available for download and require minimal technical skills to be used. Criminals also use less technical methods to steal passwords such as social engineering whereby users are deceived into revealing their passwords through a variety of techniques (Orgill, Romney, Bailey, and Orgill, 2004).

Typically internet users are not fully aware of the threats associated with using weak passwords and do not fully realise the necessity for secure password management. Users require security awareness training which should provide them with the knowledge and confidence to correctly manage their passwords (Eminağaoğlu, Uçar, and Eren, 2009).

In addition to security training, there are other authentication technologies such as multi-factor and biometrics authentication designed to enhance or even replace password-based authentication. However, adoption of this technology has moved slowly and passwords are still the most commonly used authentication technology (Herley, Oorschot, and Patrick, 2009).

1.3 The Research Questions

The study will investigate password usage habits of computer users in a personal, professional and academic context. Specific research questions to be explored are as follows:

- Are users incorporating the password practices required of them in their organisation within their own personal capacity as well?

[6] http://hashcat.net/oclhashcat-plus
[7] http://www.openwall.com/john

- Do users comprehend the dangers of using poor passwords and password habits?
- Do users have any concerns if their username and passwords are compromised?
- What is the attitude of users towards password management in their personal capacity?
- Do users know what multi-factor authentication is? Would they use it if it was provided to them?
- Are users receiving training on security awareness and password practices in their organisations? Does this appear to be adequate with regard to password security?
- How do users approach the problems associated with managing numerous user account credentials? What methods and/or technologies do they use to alleviate these problems?
- Do South African computer users have the same password habits and behaviours as others users around the world?

1.4 The Research Objectives

The objectives of this study are to gain a better understanding of why users are not employing safer practices concerning their password selection and management, particularly in their personal context. The specific objectives of this research include the following:

- To gain a better understanding of users attitudes towards their own passwords.
- To determine the level of importance given to password selection of specific resources (e.g. websites or laptop passwords) by the users.
- To determine whether password policies within organisations and institutions have a positive, negative or no effect on users' personal password habits.
- To determine if corporations and institutions provide training concerning the importance of good password management.
- To determine whether or not the corporation/institution provides the necessary tools and technologies to improve user authentication.
- To determine if there are technologies to improve access control and whether or not users will adopt these technologies in their personal capacities.

1.5 Research Statement

This study was undertaken to determine the attitudes users have towards password security and the methodology they employ to manage their passwords. The aim of this study is to determine whether or not password policies that are enforced in organisations or institutions have any influence (either positive or negative) on the users' personal password management habits.

There should be a better understanding of the significance of passwords and in which context this significance is recognised by the users for their own information. There could be a number of factors that determine this importance level ranging from users' ages to the type of information they are protecting.

It is important for users to better understand the threats and problems associated with the lack of good personal password management techniques. Users must be aware that using these techniques is not a guarantee against all possible threats but will at least improve their risk against theft of stored credentials and subsequent cracking attacks. There are various technologies that enhance the security around access control and provide improvements around managing usernames and passwords.

The study provides some insight about South African computer users relating to their password usage and attitudes towards password security. The findings in this research are compared to the findings of similar studies from other countries in an effort to determine whether or not South African users exhibit similar styles of password management habits.

The aim of the study would be to identify some of the reasons why users implement and use passwords in the manner that they do. This could provide better understanding of the challenges that users face concerning password management as well as provide feedback necessary to prompt further studies into improving password-based authentication systems.

1.6 Limitations and Scope

The research instrument that has been used in this study is an online survey. The limitations associated with using a survey method are detailed in section 4.4. This research will be limited to South African residents only. The reasoning for limiting the geographical scope is to provide a comparison against similar studies in other countries.

The participants were requested to answer the survey questions in a complete and honest manner. The survey disclaimer (See Appendix A) reiterated this request before participants partook in the survey process. The findings from the research data were therefore reliant on the accuracy of the participants' responses during the survey. All survey participants must have had experience in organising and managing usernames and passwords for computer and internet accounts. The researcher has not guided, advised or led the participants in providing answers to the questions in the survey.

There were no other restrictions placed on the survey and all internet users were encouraged to participate. The results from the survey did however indicated that nearly half (49.57%) of the participants were employed or studying in the Information Technology industry. This result may have had an impact on certain of the survey questions but the research analysis was also conducted showing a comparisons of results between the Information Technology sector and the other industry sectors.

1.7 Definition of Terms

The definition and meaning of terms used in this study are listed below:

Attackers/Cyber-criminals/hackers - A person or group of people wanting to gain unauthorised access to computer systems with the intent to steal, destroy and/or disrupt the information stored there.

Alphanumeric - Means that a password consists of both letters and numbers, i.e. a-Z, 0–9.

Common Gateway Interface (CGI) - CGI is a script or program that runs on a web server and provides dynamic content between the server and the users.

Credentials - Login credentials provide proof of identity for an individual when authenticating on a computer system. These can be in the form of a username and password.

Institution - A university where an individual is pursuing an academic study.

Participant or respondent - An individual who has taken part in this study and submitted a completed survey questionnaire.

Public-key encryption (PKE) - A method of encryption that uses a private and public key.

One-time password system (OTP) - A generated PIN or string of text used only once as part of an authentication process.

Organisation - A commercial entity, company or business at which an individual is employed on a part-time or full-time basis.

1.8 Document Structure

The remainder of this document is composed of the following chapters:

- **Chapter 2** examines previous studies related to surveys conducted about password management. The chapter also provides additional knowledge about authentication related topics including password policies, password strength and cracking, security training, authentication technologies and common password usage habits.
- **Chapter 3** provides a review and summary of previously conducted password surveys. The previous studies are ordered chronologically by date and were conducted in different countries around the world.
- **Chapter 4** details the method used for collecting and analysing the research data. This study used an online survey website to conduct the data collection process. The approach used to implement, distribute, limitations and analysis of this method are detailed in this chapter.
- **Chapter 5** contains the results from the survey data. The chapter contains the findings, analyses and summarisation of the different sections of the survey data.
- **Chapter 6** is the concluding chapter for this research. This chapter provides a summary of the findings, the conclusion of the findings and recommendations for future research.

Chapter 2

Literature Review

2.1 Introduction

To better understand the research objective mentioned in the previous chapter (section 1.4), there are several aspects about passwords authentication and there usage that needs further investigation. This chapter starts off by briefly reviewing the history of password authentication in section 2.2 and considers how it has been relied upon for the past few decades.

Password authentication is susceptible to numerous threats which include the theft, cracking and guessing of passwords. In section 2.3 these threats are detailed and discussed further. There have been a number of high profile password breaches from 2009 to 2013. Several large internet-based companies have fallen victim to these breaches, with customers' details being compromised by these attacks (see section 2.4).

Corporations have been encouraged to adopt and implement better password management into their information security policies. In section 2.5 the requirements of these password policies are discussed and as well as the problems created by the restrictions of these policies. Corporations and institutions are responsible for providing the necessary training to make their users more aware of the dangers of poor password management, which is detailed in section 2.6. The training should also improve the users' attitudes towards the password security.

Other security authentication technologies have been developed and implemented to complement or even replace password authentication. These technologies lend weight to the

idea of having more than one authentication control during the logon process which is known as multi-factor authentication. The strengths and weaknesses of these technologies are discussed in section 2.7. A well-documented cyber-attack against technology journalist Mat Honan (see section 2.8) also reiterated the failing of only using password authentication, drawing attention to the need to increase the security levels of authentication for internet and cloud computing services.

2.2 A Brief History on Password Authentication

A password is a secret string of characters (alphabetic, numeric, symbols or a combination characters) that is used to authenticate the identity of an individual and grant them access to a computer system (Saltzer and Schroeder, 1975). This type of security measure was considered essential to computer systems, especially when the computer resources were shared amongst several users.

It has been commonly accepted that the first shared computer system to use passwords was developed in 1961 at Massachusetts Institute of Technology (MIT) (Bidgoli, 2004). The problems with password based authentication were realised quite early on these systems. An example of this occurred when two administrators were simultaneously updating the password and daily message file. An error on the system caused the entire password file (with all the usernames and associated passwords) to be printed on all the consoles after the users had logged on (Morris and Thompson, 1979).

The password file or database became the primary concern for system administrators. Protecting access to the file was a high priority. This, however, was not simple to solve because access to the password file could be gained on the backup medium or through special privileged needs by system applications (Morris and Thompson, 1979). The password file, or database, was written in clear-text and if compromised could prove detrimental to the security of the system.

The idea of encrypting the password before it is written into the file was first mentioned by Wilkes (1975). The password should be converted into an encrypted string of characters and then stored in the password file in that format. When the user next logged onto the system, the encrypted string produced for the password entered would be compared to the string stored in the password file. Access to the system would be granted if the two strings matched (Morris and Thompson, 1979). This process is known as 'password hashing'.

Even if the password was stored in an encrypted format, the password system was still vulnerable to other potential attacks. The use of brute-force attacks, guessing or dictionary attacks and vulnerabilities in the cryptographic algorithm were all threats to the integrity of the passwords. These threats are discussed further in section 2.3.

Robert Morris and Ken Thompson (Morris and Thompson, 1979) formulated the concept of hashing the password using the Data Encryption Standard (DES) developed by the National Bureau of Standards (NBS). The password hashing process would be iterated (repeated) 25 times and create an 11 character encrypted string (Klein, 1990). The process also included a 'salt', two additional random characters to the encrypted password string. The salt would increase the number of potential passwords and, in doing so, the computational time for an attacker to try to crack the password (Morris and Thompson, 1979). This is the basis for the *crypt()* function that was used in most UNIX computer systems for many years (Feldmeier and Karn, 1990).

Password authentication is the most commonly used authentication process on the internet and business computer systems. The fundamentals of password security are still based on the need to securely store a user's password in a hashed (and salted) format and prevent attackers from being able to steal a password database.

2.3 Threats to Password Authentication

Passwords are vulnerable to a number of threats which can result from either technical flaws or poor password behaviour by users. Passwords can by compromised through various threat vectors including password cracking, guessing and capturing (Florencio, Herley, and Coskun, 2007).

2.3.1 Password hashing and salting

In section 2.2 the idea of storing the passwords in an unreadable or encrypted format was first conceptualised in the mid–1970s (Wilkes, 1975). To increase the difficulty of password cracking, passwords are commonly stored in an encrypted form using a hashing algorithm (Marechal, 2008).

The password hashing process produces a one-way output which is not reversible (Guzel, 2012). When a user password is created or updated, the hashing process is performed a

number of time on the input password string; this is known as the number of password hash iterations (Wagner and Goldberg, 2000). Once the password iterations are completed, the password hash output is stored in the password database. When the user next tries to login to the system, the hash output created during the login process is compared to the hash output stored in the password database; only if the two outputs match is the user granted access to the system (Wagner and Goldberg, 2000).

Password cracking tools will try to discovered the cleartext password by comparing generated hash strings with the stolen ones in the password database (Snyder, 2006). These pre-compiled lists of stolen and generated passwords are known as 'rainbow tables' and are used to match the hash value to the cleartext string (Avoine, Junod, and Oechslin, 2008). In the review of recent password breaches, RockYou.com (section 2.4.1) failed to even hash their users' passwords and were storing them in cleartext.

Unfortunately, using only hashing to secure the passwords is not adequate enough security, so there is a method of adding an additional level of strength to the password hash. The method for increasing the strength of the hashing process is to *"salt"* the password hash (Snyder, 2006). The salting process involves adding an additional variable string to the hashed password during the hashing process.

The salt must be unique for each user password and generated using a random variable which would require the hacker to try and crack each password one at a time (Brown, 2013). Linkedin had used the SHA–1[1] hash algorithm for their password database but had not salted the hash (section 2.4.5) and this ultimately led to a compromise of 6.5 million of their users' passwords.

Hash functions were designed to be fast and computationally inexpensive to generate (Merkle, 1990). This, however, is a problem, even if many iterations of the hash are used, when it comes to password hashing as generating the hash values for password strings with known hash algorithms such as MD5[2] and SHA–1 (Teat and Peltsverger, 2011). The security industry has developed algorithms that are computationally and/or memory intensive to process such as Password-Based Key Derivation Function (PBKDF2)[3], bcrypt and scrypt[4].

Password-Based Key Derivation Function (PBKDF2) introduced the idea of key stretching (Kaliski, 2000) whereby the output from each of the hashing iterations would be used on

[1] http://www.ietf.org/rfc/rfc3174.txt
[2] http://www.ietf.org/rfc/rfc1321.txt
[3] http://tools.ietf.org/html/rfc6070
[4] http://tools.ietf.org/html/draft-josefsson-scrypt-kdf–00

the next hashing iteration and this would be repeated over and over (Brown, 2013). This type of hashing can increase the security strength as the number of iterations of the password hashing is increased.

Attackers have harnessed the power of modern graphics' Graphics Processing Unit (GPU) to crack huge sets of passwords in short periods of time (Kingsley-Hughes, 2011). These processors are relatively low cost, have high speed memory and clock speed and run millions of computations per second (Shaw, 2013). Many graphics cards can be inserted into a single computer and the cracking software is able to utilise all the GPUs in parallel (Roberts, 2012).

An implementation that used the concepts from PBKDF2 was bcrypt (Provos and Mazieres, 1999). Bcrypt uses the blowfish algorithm (Schneier, 1994), an expensive computational encryption algorithm along with a configurable iteration value to provide a strong hash algorithm that slows down the attacks from password cracking tools. Bcrypt also uses memory-based lookup tables which are constantly modified during the hashing process; this proves to be problematic for GPU-based cracking and therefore hinders the process of using such an attack.

The recently drafted algorithm called scrypt uses a memory hard function for its password hashing process (Percival, 2009). The algorithm will use large amounts of random access memory (RAM) posing a problem for GPU-based cracking which is designed to take advantage of the computational power of the GPU and not the memory capabilities of the computer.

2.3.2 Brute-force and Dictionary attacks

The password guessing attack is a process whereby different passwords are repeatedly used to gain access to a user account. These types of attacks can be automated and are typically brute-force, dictionary or a combination of both (Florencio *et al.*, 2007).

Brute-force attacks are conducted by attackers by trying different combinations of characters (Kedem and Ishihara, 1999). The combination of characters can be composed of different character types and character lengths. These attacks can be quite time- consuming and computationally taxing. GPU-based password cracking has significantly improved the speed at which brute-force attacks can be conducted

Dictionary attacks can be done both online and offline (Pinkas and Sander, 2002). Online attacks can be initiated using a large list of passwords and running repeated login attempts

using the list of passwords but are easily detected on monitored computer systems. Offline dictionary attacks are performed against a comprised and captured password database which is difficult to defend against if the password database has been stolen.

Protecting against brute-force and online dictionary attacks can be accomplished by employing a number of security controls. User accounts can be locked out after a certain number of attempts Pinkas and Sander (2002) (Gold, 2010). The use of a delayed response, while not complete deterrence, could slow down an online attack and frustrate an attacker by stagnating the attack session. There are, however, problems associated with using account lockout controls. As mentioned in (Pinkas and Sander, 2002) attackers could launch an ongoing denial of service attacks against a website and lock out thousands of users accounts, effectively making the website unusable. The use of a stronger hashing algorithm such as bcrypt or scrypt will slow the attack of the hackers down considerably due to their high memory and computational usage.

Defending against offline dictionary attacks is primarily focused around protecting the password database. Access to the password database should be limited to only the system administrators and security personnel. The salting of the hash also improves the protection of the password database against these attacks. In section 2.4 there are breaches which involved the theft and then offline attack against the dictionary database. Both Stratfor (section 2.4.3) and Adobe Systems (section 2.4.7) have fallen victim to this attack.

Another counter-measure that could be employed to protect against brute-force and dictionary attacks is a proactive password checker (Klein, 1990). A password checker can verify the strength of a user's password by evaluating the length, complexity and previously used password history. The password checker will alert the user if the password does not meet minimum requirements or has been previously used. The password checker could use a similar technique as password cracking tools by comparing the password to a dictionary list of words (Bishop and Klein, 1995). The password checker can also test the strength of a password's complexity (Wiberg, 2011) (Moshe, 2011) by analysing the composition of the password and determining its calculated strength (Yan, 2001).

2.3.3 Social Engineering attacks

Capturing of cleartext passwords is often the simplest way for a user's credentials to be compromised. Users can inadvertently disclose their passwords to an attacker technical, social or combination of techniques such as keyloggers (Howard and Hu, 2012), social engineering (Peltier, 2006) and phishing.

Keyloggers are one such technical tool used to steal users' passwords (Kahate, 2013). A Keylogger is malicious software that monitors and logs all the keyboard inputs from a user's activity. Attackers are then able to retrieve these logs and use the information to compromise the user's accounts.

Criminals may engage in more social behaviour in order to solicit passwords from users, an approach referred to as social engineering (Peltier, 2006). The perpetrator can acquire a user's password by pretending to be an IT staff member of a company, watching the user enter their password, reading the user's password from a notepad and using a phishing email or website.

Hackers could use a combined social engineering and technical attacks known as phishing to deceive victims (Badra, El-Sawda, and Hajjeh, 2007). Attackers will send targeted emails to users trying to direct them to fake internet websites. The users will then be asked to enter their user credentials into the fake website thereby providing the attacker with usernames and passwords. Criminals may also send malicious software such as keylogger in order to steal personal information.

These types of social attacks are quite common and are easy to perform, even with limited technical knowledge. Defending against these attacks requires the use of some defensive software and technologies such as web client enhancements, phishing blacklists, malware scanners for email and websites and multi-factor authentication (Badra *et al.*, 2007), (Berghel, Carpinter, and Jo, 2007). It also requires the co-operation and awareness training of computer users (Adams and Sasse, 1999).

2.3.4 Poor password practices

Users should have both knowledge and clear understanding of these security threats. They should be motivated to continually be aware of these threats and not engage in insecure behaviours that could lead to their username and password being compromised (Adams and Sasse, 1999).

Users' habits when managing passwords can also affect the security of their passwords. Users have been observed writing down their passwords on scraps of paper or in notebooks (Summers and Bosworth, 2004) (Zviran and Haga, 1999). This practice makes the password available to anyone that can simply read and also increases the likelihood that the password may be forgotten if the paper is discarded or lost.

2.3.5 Password Reuse

Users will often reuse the same password across multiple accounts in order to simplify the need to recall numerous passwords. The article "The domino effect of password reuse" (Ives, Walsh, and Schneider, 2004) describes how cyber-criminals can use one set of stolen credentials to compromise other accounts of a user, if indeed that user reused the same password on their other accounts. In the section 2.8, a Wired.com journalist suffered an attack that was perpetrated by compromising one account after another in a daisy-chained approach.

The authors Ives *et al.* (2004) suggest that such an attack is quite likely and could be dispatched in a similar manner to a denial of service attack (Mirkovic, Hussain, Wilson, Fahmy, Reiher, Thomas, Yao, and Schwab, 2007). These attacks could allow the perpetrators gain access to a user's accounts one after another. These types of attacks could be automated and could include a sizeable list of stolen user credentials.

An incident was reported on the Carnegie Mellon CERT website (Carnegie Mellon University CERT, 1998). The incident reported that a hacker had been storing and decrypting a large number of stolen password files on a breacher server. The hacker was using password cracking software to decipher the encrypted passwords. A compelling discovery during this investigation was the fact that the stolen passwords did not originate from the compromised server that they were on. Rather the list of passwords had been gathered from a number of sites and would indicate that the perpetrator was building up a collection of stolen passwords.

The analysis and results on the Sony password breach (see section 2.4.2) by researcher Troy Hunt confirmed the researchers suspicions that internet users of these vendor websites were practicing poor password security (Hunt, 2011). Their passwords were short, were often composed of dictionary words, were not complex in form or randomness and were being reused on both Sony databases (Hunt, 2011). The researcher also revealed that the same user accounts in the Sony database were reusing the exact same password on the Gawker password database (Raphael, 2010).

The habit of reusing the same password across multiple accounts can be attributed to the fact that users see this as the easiest way to memorise their passwords (Gaw and Felten, 2006). The study was undertaken to quantify the reuse password rate and reasons for this by users. The laboratory portion collected metrics of password usage by means of website and Common Gateway Interface (CGI) script which presented the participants with a

list of websites. The second portion of the study was composed of a questionnaire that posed questions about participants' reasoning for their password management methods. The researchers provided a quantified calculation of password reuse and their laboratory study showed that respondents are regularly reusing the same password across multiple accounts. Their reason for doing so is mainly due to the fact that it is easier to remember one password as they have many user accounts to manage.

The recommendations to reduce the reuse of passwords includes implementing additional security technologies such as smart cards and tokens (Ives *et al.*, 2004). Users should also receive security training concerning the dangers of password reuse, and software tools such as password manager should be introduced to assist in reducing the rate of reuse (Hunt, 2011) (Schneier, 2010) (Gibson and Laporte, 2010).

2.4 Recent Data and Password Breaches

In recent years there have been high profile data breaches from a number of internet companies. These companies - including Sony, Linkedin and Yahoo - have had their customers' password databases stolen and their passwords have been disclosed to the public.

2.4.1 RockYou.com, December 2009

In December 2009, it was revealed that the social gaming company called RockYou[5] had fallen victim to a massive data breach (Siegler, 2009). The site had been breached using an SQL injection attack and 32 million user accounts and passwords were stolen (Leyden, 2009). Further analysis on the breach revealed that the company had been storing the customers' passwords in cleartext and had implemented a weak password checker which limited the number of characters and character types that could be used (Cubrilovic, 2009). The customers were using poor password selection and an analysis of these passwords showed that three common passwords used were "123456","12345" and "123456789" (Leyden, 2010).

[5]http://rockyou.com/ry/home

2.4.2 Sony Playstation Network, April 2011

The Sony Playstation Network[6] was attacked in April 2011 and 77 million customers' records - including passwords - had been stolen (Baker and Finkle, 2011) (Peckham, 2011). Sony took the entire Playstation Network offline and customers were unable to login and change their details. When the services were eventually restored, customers were required to change their passwords to their Playstation network accounts (Rashid, 2011). Sony suffered a number of cyber attacks during 2011 including the theft of another million customer passwords by hacker group LulzSec using an SQL injection attack on SonyPictures.com (Albanesius, 2011). The subsequent remediation and repairs to their systems cost Sony corporation in excess of 171 million US dollars (Schwartz, 2011).

2.4.3 Stratfor, December 2011

Research and analysis company Stratfor[7] had its website compromised in December 2011. As a result 75,000 customer details were stolen and published on the internet (Perlroth, 2011). A further 860,000 password hashes were leaked from the registration database onto the internet (O'Dell, 2012). Hactivist group 'Anonymous' claimed responsibility for the attack and posted the stolen information on the Pastebin website. Analysis into the types of passwords used on the registration database revealed that weak passwords were used (Rashid, 2012). Security researchers used the Hashcat[8] password 'hash cracker' in combination with a list of dictionary words, words from the Bible and previous crack password lists to discover the passwords (Ragan, 2012). Users were commonly using personally identifiable information in their passwords such as birthdays, names of family or friends, and even private references to formulate their passwords (Rashid, 2012).

2.4.4 YouPorn, February 2012

Youporn is a large adult content website that suffered a security breach in February 2012 (Cluley, 2012). The attackers were able to able to steal the unencrypted chat log file from an insecure directory on the public website of the YouPorn chat service and published them on Pastebin (Yin, 2012). The company had not implemented proper security practices

[6] http://us.playstation.com/playstation-plus
[7] http://www.stratfor.com
[8] http://hashcat.net/hashcat

by storing the log files in cleartext and had not provided controlled access to the logs. While only 6400 passwords were believed to be leaked (Schroeder, 2012), the website is one of the most popular in the world; consequently there was major embarrassment for the users whose contact details were exposed (Didymus, 2012).

2.4.5 Linkedin, June 2012

The professional social networking website Linkedin[9] had an estimated 6.5 million user passwords leaked onto the internet in June 2012 (Kitten, 2012). Linkedin had stored the passwords in a hashed format but had failed to salt the hash when storing the users' passwords (Kamp, 2012). Hackers and security analysts quickly went to work trying to crack the hashed passwords; again it was revealed that user passwords were extremely weak and common (Kelly, 2012). The passwords "link", "1234", "work", "god" and "job" were top of the list of the 30 most common passwords used.

2.4.6 Yahoo, July 2012

Yahoo experienced a password breach of about 450,000 users on their Yahoo Voice website[10] (Kaplan, 2012). In July 2012 hackers were able to obtain the customer credentials using a URL based SQL injection[11] attack and again the passwords were not stored in an encrypted format (Fitzgerald, 2012). A prominent security company (Rapid 7) conducted an analysis on the leaked password database and provided breakdown on the number of effected customers and the email service provider they were using. The initial report stated that only Gmail and Yahoo customers were effected however the security companies' report stated that customers were using email addresses from many of the largest email providers including Yahoo, Gmail, Hotmail, AOL and Comcast (Walton, 2012) and demonstrated that the effect of this breach was more widespread than initially thought.

2.4.7 Adobe Systems, October 2013

In October 2013 Adobe Systems[12] announced that their network had been breached (Krebs, 2013). Attackers had managed to steal the source code for several of their software

[9] https://www.linkedin.com
[10] http://voices.yahoo.com
[11] http://kyrionhackingtutorials.com/2012/01/url-based-sql-injection
[12] http://www.adobe.com

applications as well as information about their customers, including their usernames and passwords. The hackers managed to steal a 9.3 gigabyte password file containing 130 million username and passwords, and published it on the internet (Goodin, 2013b). Adobe software engineers chose to use a Triple DES encryption cipher rather than hashing the passwords (Kale, 2013). The problem with encrypting versus hashing is that encryption is designed to be reversible and possessing the encryption cipher key allows passwords to be decrypted. Electronic book (ECB) mode, used when encrypting the passwords, is known to reveal information about the password in the encrypted format (Kale, 2013). The Adobe engineers also used the same cipher key for encrypting each password. It is not clear whether or not the perpetrators managed to steal the cipher during the breach. An anonymous list of the top 100 passwords claimed to be from the Adobe attack has appeared online[13].

Cyber attacks and password thefts from major internet websites have been prolific and all too common in recent years. Prominent companies such as Linkedin and Adobe have had millions of customers' details stolen and leaked onto the internet. While certain recipients of these attacks such Sony were part of an ongoing attack against the company, cyber-criminals did not discriminate against any particular type of company, as was demonstrated with the Youporn and Stratfor attacks. The sheer number of accounts being harvested during these attacks is quite concerning and is shown in the Figure 2.1

2.5 Password Policies and Best Practice Guidelines

Organisations and educational institutions typically include a restrictive password policy as part of their information security password policy implementation. Password policies are implemented with the intention of imposing restrictions on users concerning password creation, usage and reset.

2.5.1 Password policy standards

The United States National Institute of Standards and Technology (NIST) (Scarfone and Souppaya, 2011) and United States Department of Defense (Brand and Makey, 1985) both published papers that provide guidance for implementing controls for a password policy within organisations and for various types of threats against passwords. These papers

[13]http://stricture-group.com/files/adobe-top100.txt

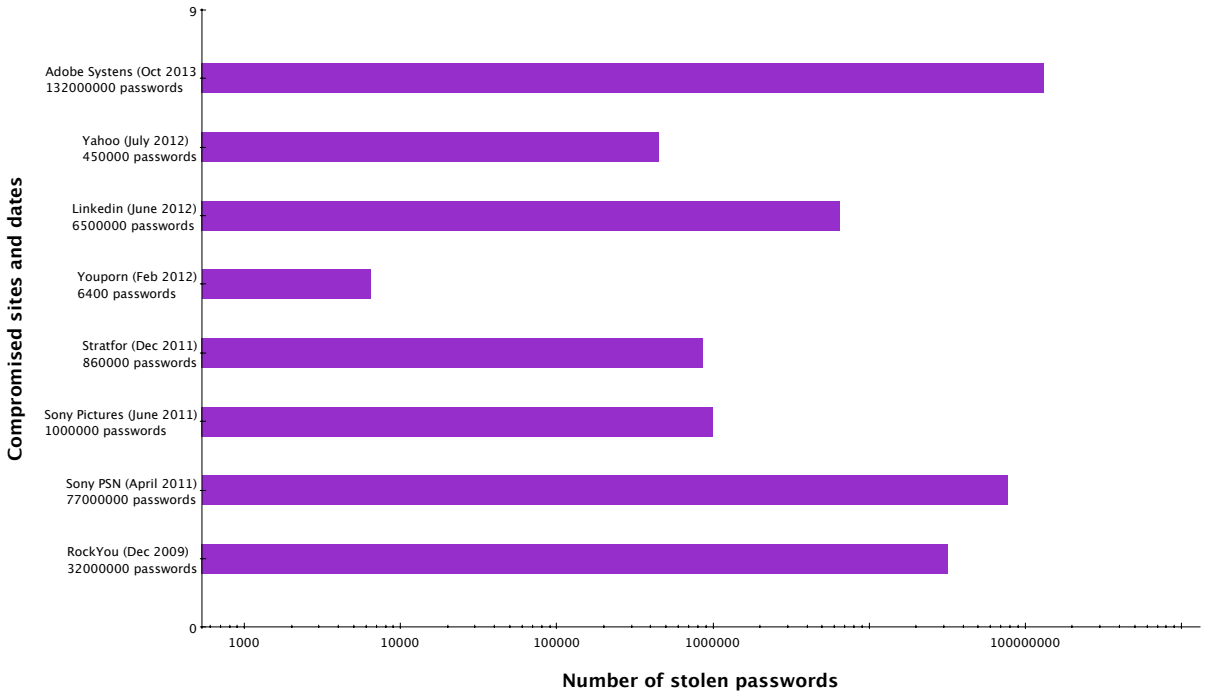

Figure 2.1: A timeline of notable password breach attacks

suggest several controls for compliance with their recommendations such as password management systems, password issuance and resets and strategies for simplifying password management for users.

In order to comply with these requirements, password policies include minimum requirements on the number of characters and a minimum level of complexity. Password strength is determined by its resistance to password cracking and guessing. Two attributes that increase password strength are the length and complexity of the password (Wood and Shield, 2008). An example of this would require a user's password to have a minimum of eight characters. These characters need to be composed of at least one numeral and have both upper and lower case characters. Stronger passwords are less vulnerable to attacks such as brute-force attacks. This is discussed in more detail in section 2.3.

These two publications also provide information about account lockouts and password resets. Computer systems should lock a user account after a certain number of failed login attempts. The account should remain inaccessible until the password has been reset upon request from the user. This control can mitigate against guessing attacks. A password reset can be accomplished by visiting the Information Technologies Department of the organisation or by implementation of an automated password reset system (Scarfone and Souppaya, 2011).

Password expiration and password history are additional controls that can be implemented into the password policies (Wood and Shield, 2008) (Brand and Makey, 1985). Users can be prompted to change their password on a regular time and interval. Password history keeps track of previously used passwords on the system and prevents users from reusing the same password that has already been used.

2.5.2 Password policy concerns

Password policies have come under some scrutiny from other studies as well. One article provides interesting results on how the enforcement of password policies in the corporate environment is causing the users to practice bad password management (Summers and Bosworth, 2004). The users are required to remember more complex passwords as well as being forced to change these passwords on a regular basis. This inadvertently sways users to use poor password management such as writing passwords down on paper and storing them next to or on computer desktops (Komanduri, Shay, Kelley, Mazurek, Bauer, Christin, Cranor, and Egelman, 2011).

A password policy is a necessity for businesses; however, it is essential that the users who need to comply to this policy are educated in understanding the reason why the policy has been selected and what the threats are when poorly managing and selecting their passwords (Summers and Bosworth, 2004). The lack of user security awareness training is detailed in section 2.6.

Managing passwords and adhering to an organisation's passwords comes at a cost of time (Inglesant and Sasse, 2010). The task of coping with creating, changing frequently and remembering longer and more complex passwords is a hindrance on users' productivity. The researchers suggest that password policies need to be more flexible and that the needs of different groups of users within an organisation can be subject to varying restrictions depending on their security risk level. Organisations should be implementing a password management system that meets the requirements of security compliance but also provides the usability that allows users to maintain a certain level of productivity.

Research studies have also shown that different frameworks for password authentication provide assurance level based on the risk and sensitivity level of the system or application (AlFayyadh, Thorsheim, Jøsang, and Klevjer, 2012). These frameworks were compared to the current password policies that have been implemented by a number of websites and organisations. The results indicated that there is no consistency in the password

requirements or restrictions amongst the organisations and no indication of them having implemented an authentication framework. A number of the sites employed extremely lenient password policies and were not completely enforced. Authentication frameworks are considered a far better approach to defining a consistent and risk mitigating policy.

Another approach to creating a password policy could be to use a password policy simulation tool (Shay and Bertino, 2009). The simulation tools is able to build a model for an organisation's password policy by incorporating the users, the list of services the users access, and defining a risk level to that user, password strength, the probability of password attacks and the cost associated with a service being comprised or unavailable for a specified period of time. Organisations could use this simulation for modelling offline and require little or no user input.

2.6 Security Perceptions and Awareness Training

Researchers conducting studies about password behaviour and habits often try to gauge the attitudes and perceptions of the participants concerning password security.

It has been observed that users often express an indifferent attitude toward password security and are frustrated by having to comply with an enforced password policy (Komanduri *et al.*, 2011) (Shay, Komanduri, Kelley, Leon, Mazurek, Bauer, Christin, and Cranor, 2010) (Albrechtsen, 2007) (Inglesant and Sasse, 2010) (Weirich and Sasse, 2001) (Adams and Sasse, 1999). Users will often resort to using poor password management habits such as reusing passwords, writing down their passwords and finding way to circumvent the controls within a password policy. Information security and the associated policies are considered overly time- consuming and thus an inhibitor of productivity.

It has been observed that users demonstrated a lack of interest for partaking in security awareness training (Hart, 2008). The users believed that their individual risk was low and that they would not be personally targeted for attack. The users are often negatively motivated when companies suggest or impose penalties on them for failure to comply with the security policy (Herath and Rao, 2009). Personal accountability is not considered to be a serious concern amongst users (Wylder, 2003) as they assume they can rely on their colleagues to support them when a password policy has been breached (Weirich and Sasse, 2001).

Users that exhibit a sense of understanding of security awareness are considered to be paranoid or "geeks" (Weirich and Sasse, 2001). These users are seen as "pedantic" and

"anal". They are also considered to be very unsocial people as they refuse to share their passwords with their colleagues.

Certain demographics of users exhibit a better understanding of password security and ultimately comply to the requirements of an organisation's password policy (Shay *et al.*, 2010) (Duggan, John-on, and Grawemeyer, 2012). These users were predominantly from the Information Technology sector or students of Computer Science. Users that were better educated in the aspects of security and more specifically, password security, had less resistance to password policy restrictions.

Security awareness training is an essential requirement for educating users and informing them of potential threats concerning information security. In the article "Building an Information Technology Security Awareness and Training Program", the author states *"If people are the key, but are also a weak link, more and better attention must be paid to this "asset.""* (Wilson and Hash, 2003). Organisations should focus on educating people with knowledge which is undeniably more important than focusing on technology to protect them (Desman, 2003). Training should be ongoing and users should be encouraged to attended "refresher" courses on a regular basis.

More specifically relating to the password security training (Wilson and Hash, 2003), users need to be taught fundamental key points when creating passwords, the reasons for frequently changing passwords and the necessity to protect their passwords from possible disclosure.

Studies such as Adams and Sasse (1999) and Weirich and Sasse (2001) have often referred to the lack of understanding and training provided to the users as a common cause for users' poor password usage practices. Personal accountability and concern about disclosing their passwords should be part of the mind-set users should incorporate into their password usage habits (Albrechtsen, 2007).

2.7 Security Authentication Technologies

Security vendors have developed numerous authentication technologies to improve security vulnerabilities and threats associated with password authentication. These technologies can be either complementary or can replace password-based authentication all together.

There are a number of alternate and/or complementary authentication technologies to passwords (Ives *et al.*, 2004). These include public-key encryption (PKE), public-key

infrastructure, biometrics, smart cards or tokens and single sign-on technologies (SSO). However, these technologies have not been incorporated by companies mainly due to cost, complexity, or both.

Multi-factor authentication is the process whereby a user requires two or more elements of authentication in order to successfully complete the authentication process (Hayden, 2013). These authentication factors can be based on different users' credentials such a knowledge-based factor which is something a person knows (password or a PIN), a possession-based factor which a person possesses (a token or smart card), or a personal attribute factor which is a physical feature (fingerprint or voice analysis). A combination of these factors is frequently used as part of the authentication process.

2.7.1 Public-key encryption and Public-key infrastructure

Public-key encryption provides the user with private and public encryption keys. The private key is stored on the user's computer or smart card and is used to send encrypted authentication requests to a server (Needham and Schroeder, 1978). The server does not need to refer to a password file or database as it can verify the users with the public key and thus eliminate a threat of password file theft. The threat vector is solely on the private key and where it is stored.

Public-key infrastructure will allow authentication with the user's private key across many systems and applications. This technology allows the user to have access, without the need of a password, to external and third party systems that integrate their systems with the public-key infrastructure (Kuhn, Hu, Polk, and Chang, 2001). PKI also has the ability disable a user's private key through a key revocation facility. These PKI systems are notoriously complex and difficult to implement, often improperly implemented and eventually abandoned by companies (Mattila and Mattila, 2006).

Companies have failed to successfully install a PKI solution because they find the implementation complex and the systems not flexible enough to meet their needs (Mattila and Mattila, 2006). These solutions also tend to be become costly not only to implement but also for ongoing administration (United States General Accounting Office, 2001).

2.7.2 Biometrics

Biometrics is another authentication technology (Das, 2005) which can be used for authentication and access control. Using a physical feature of a person - be it a fingerprint, eye scan or voice recognition - could be a replacement for a password because these physical attributes are unique to that person. The main purpose of authentication is that individuals identify themselves to the system in order to gain access; biometrics-based authentication truly identifies the individual based on physical attributes that are unique to each individual (Matyás Jr. and Riha, 2003). Passwords and/or security devices (smart cards and tokens) are simply things that an individual has or knows. There are, however, methods that can be used to steal a digital copy of these attributes using network analysers. Unlike private keys, they cannot be changed or revoked (Ives *et al.*, 2004).

2.7.3 Smart cards and tokens

Smart cards and tokens can provide users with an alternate approach to authentication and system access. Smart cards can store private keys and passwords. Smart cards have computation abilities to create encrypted messages for the public-key encryption process (Aussel, 2007). The users must retain possession of the smart card in order to retain security of this solution.

2.7.4 Single sign-on

Single sign-on (SSO) is a technology mechanism that enables users to authenticate once with a single username and password in order to gain access to multiple systems and applications (Pashalidis and Mitchell, 2003). The benefits of such an authentication process enables the users to manage only one set of user credential and gives the security administrators the right to revoke access to all systems and applications by disabling or deleting that user's account. A drawback of single sign-on technology is its inability to integrate with legacy applications and systems (Chinitz, 2000).

2.7.5 Password managers

Password managers have been developed to ease the process of managing multiple user accounts, create unique passwords for each account and store them in a secure manner.

Password management software is a *"vault"* for storing and recalling users' collections of passwords (Burnett and Kleiman, 2006). Password managers usually require the user to create a master password that grants access to the collection of passwords. Password managers have password generator features which allow the user to create randomly composed and length passwords (Mannan and van Oorschot, 2012).

Password managers have been observed to present usability issues for users as they find them to be a non-essential part of their workflow and authentication habits (Chiasson, van Oorschot, and Biddle, 2006). Users have also demonstrated a distrust for password managers, in particular the ones that store the password database online (Karole, Saxena, and Christin, 2011). Users preferred using password managers that were available on their mobile phones instead of USB or online-based managers.

Examples of two popular password managers are Keepass Password Safe[14] and LastPass[15]. Both applications provide the same fundamental requirements of a password manager which is to securely store user account credentials. The two applications differ in the fact that Keepass keeps the password database locally on the computer while Lastpass stores the database online.

Keepass is installed on a computer hard drive or on a USB flash drive along with the password database. According to the Keepass features webpage[16] passwords are stored in an encrypted Advanced Encryption Standard[17] (AES) and Twofish[18] database. Access to the database is controlled by using either a master password which is hashed using SHA–256[19] or by using a key file that needs to be presented at login, or by using a combination of both a password and a key file. The output from the hashed master password is used as the private key to encrypt the database.

The Keepass interface is used to create groups of user credentials. The groups can store multiple entries for websites, email addresses, banking details or any other authentication credentials the users specify. The username or password can be copied into the operating system clipboard by double clicking or right clicking on the entry in the password group. This is demonstrated in the Keepass screenshot Figure 2.2. The operating system's clipboard can be configured to be regularly flushed and cleared by Keepass settings.

[14] http://keepass.info
[15] https://lastpass.com
[16] http://keepass.info/features.html
[17] http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
[18] https://www.schneier.com/twofish.html
[19] http://tools.ietf.org/search/rfc4634

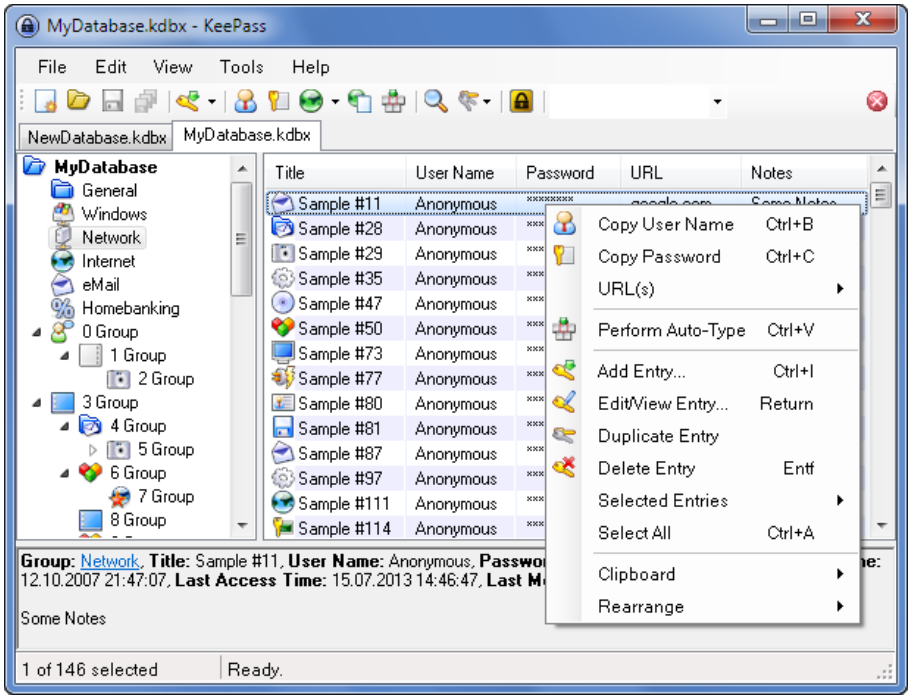

Figure 2.2: Keepass user interface screenshot

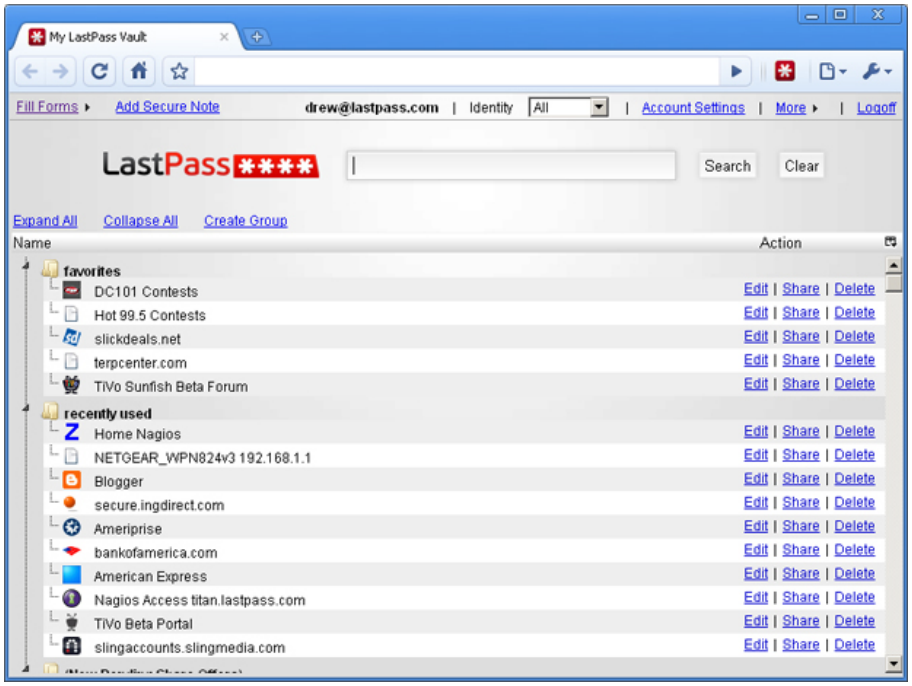

Figure 2.3: Lastpass user interface screenshot

Keepass does not have an official version that is supported on mobile smartphones. There are, however, numerous unofficial ports[20] of the software that run on various smartphones including Blackberry[21], Android[22] and iPhone[23].

Lastpass provides a free version of its software or a subscription[24] based password management service known as Lastpass Premium[25]. Lastpass is supported on multiple operating systems and access to the password database is provided through the use of browser extensions. Lastpass supports many of the most popular internet browsers including Microsoft Internet Explorer, Chrome, Safari and Firefox. The Lastpass password database, encrypted using 256-bit AES encryption, is only ever decrypted locally[26] on the user's computer.

Lastpass allows the user to gain access to their password "vault" using their internet browser; similarly to Keepass, it presents the user with the groups of user credential entries. Passwords and/or usernames are also copied to the clipboard when the user right clicks on the entry of choice. The Lastpass user interface is shown in the Lastpass screenshot Figure 2.3.

Lastpass provides additional benefits to its premium service users, including a mobile version that runs on all the major smartphone platforms and integration with other multi-factor technologies such as Yubico Yubikey[27] and Google Two-Step Verification[28]

2.8 Authentication Failure: Mat Honan's Epic Hack

Mat Honan is a writer for Wired[29] magazine. In August of 2012 he was the victim of a targeted cyber attack which led to the complete compromiise of all of his online services and accounts (Honan, 2012). This case study is not entirely centred around the password authentication habits of Mat Honan but rather demonstrates the techniques that can be

[20] http://keepass.info/download.html
[21] http://appworld.blackberry.com/webstore/content/131133/?countrycode=ZA&lang=en
[22] http://www.keepassdroid.com
[23] http://minikeepass.github.io
[24] https://lastpass.com/go-premium
[25] https://lastpass.com/features_premium.php
[26] https://lastpass.com/how-it-works
[27] http://www.yubico.com
[28] http://www.google.co.za/landing/2step
[29] http://www.wired.com

used to circumvent password authentication and the need to provide improved access control technologies for protecting 'private information' stored in the cloud.

The hackers that perpetrated the attack were motivated by a single goal - to take control of Mat's Twitter account. One of the hackers involved in the incident claimed that they simply wanted his Twitter handle (@mat) and that all the other peripheral damage that they caused was simply "gravy" (Honan, 2012). The "gravy" that the hacker was referring to included the deletion of Mat's Gmail account, the hacking and abuse of his Twitter account, and the remote wiping and deletion of all content off his Macbook, iPad and iPhone. This left Mat's digital status and content in complete disarray.

While the motive for the attack was quite simple, the preparation and execution of the attack was well-planned and carried out with precision. The hackers (one of whom identified himself later as Phobia) began their attack by performing some basic reconnaissance about their target: Mat Honan. They determined from Mat's personal website[30] that he used his Gmail account (mhonan@gmail.com) to login to his Twitter account and they used this Gmail email address on the Google account recovery page[31].

The Google account recovery page allows users that have forgotten their password or account name to reset or recover the details of their account. If the user does remember their account name but is unable to remember the password, there is an option to send an email to a previously configured email address. The recovery email address is shown on the browser but it obscured in certain parts of the email with asterisk symbols. In the case of Mat's Gmail account recovery, his recovery email address was displayed as "m●●●●n@me.com". The hackers quickly realised that this email address was probably mhonan@me.com, an Apple ID[32] email address.

The hackers now knew Mat had an Apple ID account and if they could access this account, they could send the Gmail recovery email to this email address. A note mentioned by Mat Honan (Honan, 2012) at this point is that Google provide their users with a multi-factor authentication option called 2-Step Verification[33]. This additional security measure required users to not only provide their username and password but also provide a one-time generated PIN from their Google Authenticator application on their mobile device during the login process. If Mat had 2-Step Verification enabled, it is possible that this attack would have been cut short at this point.

[30] http://honan.net
[31] https://www.google.com/accounts/recovery
[32] https://www.icloud.com
[33] http://www.google.com/landing/2step

The attack did, however, continue and the hackers now had to gain access to Mat's Apple email account. This is where the hack became a bit more complex. In order to gain or recover access to an Apple account through Apple's technical support, the person needs to provide a billing address and the last four digits of their credit card. Acquiring the billing address was a relatively simple task. The hackers were able to find these details on the internet using a whois[34] lookup search on the domain name of his personal website.

The credit card details were more difficult to attain. The hackers phoned Amazon[35] and told them that they wanted to add a new credit card to their account for billing services. In order to accomplish this, the caller needed to provide Amazon with the name of the account holder, a billing address and an email address registered with the account. The hackers provide all these details (which had already been acquired) and presumably added a fake credit to Mat's Amazon account. The hackers then ended the call.

The hackers then called Amazon back to report that they were unable to access their user account (Mat Honan's Amazon account). The hackers had to provide the Amazon support with their name, the billing address and the recently added credit card number in order to have an additional email address added to the recovery and reset option. They then proceeded to the Amazon website and sent a password reset to the newly added recovery email address. This allowed the hackers to now view the last four digits of all the credit cards associated with Mat's Amazon account. This was all the information they needed to gain access to Mat's Apple account.

Now armed with the name, billing address and the last four digits of Mat's credit card, the hackers contacted Apple support service and reset the password to his mhonan@me.com account. This finally gave the hackers complete access and control over Mat's internet services and content. The hackers now reset the password to Mat's Gmail account by sending a recovery email to his Apple email account, thereby giving them access to his Twitter account. They deleted the contents of his entire Gmail inbox and wrote profanities and racist comments on his Twitter account timeline.

Mat had also enabled the "Find My iPhone, iPad and Mac[36]"" service on his Apple account. This service allows Apple users to locate their devices in the event of loss or theft. The service also allows the user to remotely wipe all the contents from the devices - and that is exactly what the hackers did. All of Mat's content on his Macbook was erased and he was unable to logon to it. Both his iPhone and iPad were reset to their

[34]http://www.whois.com/whois/honan.net
[35]https://www.amazon.com
[36]https://www.apple.com/icloud/find-my-iphone.html

factory default settings. Unfortunately for Mat he had also failed to make a backup of his Macbook and he lost countless sentimental photos of his family.

This cyber-attack highlighted the flaws in the security processes at both Apple and Amazon. Both companies have subsequently changed their policies and amended the vulnerabilities that were exploited in this attack. Apple no longer accepts password changes over the phone (Chen, 2012) and Amazon no longer allows additional credit cards to be added over the phone (Olivarez-Giles, 2012).

From an authentication perspective, the attack on Mat Honan highlights a key failing in the current password-based authentication environment on which most of the internet and cloud services are based. A secondary and possibly tertiary authentication step, such as Google's 2-Step Verification, will improve the security authentication process and should be implemented as a mandatory requirement when logging onto an internet service.

Mat also used the same user account (his Gmail account) as the primary email address for most of his services such as Twitter and Amazon. When the hackers compromised this single account, they then had the proverbial keys to his digital kingdom and were able to pretty much destroy everything connected to it. Many internet users will likewise use the same user account as their primary contact and/or authentication account to a number of their internet and cloud services. Protecting this single account, then, is of utmost priority and password-based authentication is not enough of a security measure in the era of cloud-based computing.

2.9 Summary

This chapter has detailed the background of password authentications. The idea of password-based authentication was first conceptualised and then implemented in order to force system users to identify themselves for the purpose of gaining access to computer resources.

Over the past few decades, there have been numerous threats and vulnerabilities discovered affecting password authentication. These have, unfortunately, been exploited in many high profile password breaches. Companies have been encouraged to implement password policies and best practice policies in order to prevent their users' passwords from being compromised. Furthermore, these companies should be providing their users

with awareness training and pertinent technologies necessary to cope with the task of managing numerous user account credentials.

Unfortunately, users' attitudes towards password management is poor and they often consider these security measures more of a hindrance to their productivity than a benefit. Users tend to employ bad password habits in order to simplify their password management or even entirely circumvent security controls that have been implemented.

Alternate authentication technologies have been designed to integrate with or simply replace password authentication. The use of multi-factor authentication enhances the security process for identifying and authenticating the users on computer systems. Password management tools have also been developed to aid computer users in securely storing and retrieving their passwords for large numbers of user credentials.

There have been a number of similar survey studies conducted in different countries. The details and outcomes of these studies are presented in the following chapter (Chapter 3).

Chapter 3

Related Works - Password Surveys

3.1 Introduction

In recent years, there have been a number of password management and usage surveys conducted around the world. These studies have sought to identify the everyday password habits of computer users, including the types of passwords being created, the methods for storing and recalling passwords and the reasons why users have sought to use these identified methods. This chapter summaries six significant published studies from around the world.

3.2 University of Canberra, Australia, 2006

Researchers from the University of Canberra in Australia conducted a survey to determine the attitude of its respondents towards the security of passwords (Bryant and Campbell, 2006). The researchers decided to question students from the business faculty of the university as these would represent a sample that were non-specialist in Information Technology and would display behaviour more indicative of employees in a corporation. In total, they had 884 respondents take part in the study.

The researchers decided to focus primary on email usage and email habits of their participants as email was considered by them to be the most widely and frequently used application. Over 70% of the respondents had two to three email accounts to manage. From the demographic data collected in the survey, 66% of the recipients were between

the ages of eighteen and twenty-five. Over 90% of the respondents were full-time students and 60% were part-time employees. Over half of the respondents (54.3%) had between six and ten years of experience with computers.

The respondents most commonly chose to use between six and eight characters to generate their passwords (54%). The results of the password composition questions indicated that 39.4% used alphabetic character only and 42.3% used alphanumeric characters only. Only 4.1% used special characters in their passwords. 43.1% of the respondents used relatable information in their passwords such as nicknames, street names or a registration number. Over sixty percent (61.9%) indicated that they never change their passwords and 60.9% percent also admitted that they had also forgotten their password.

The survey results indicated that over half (56.1%) of the respondents either use the same password or a similar password on all their email accounts, while 37.5% of the respondents also indicated that they reuse the same or similar passwords on other applications that they use on their computers. The majority of the participants (52.7%) responded that they did not share their passwords with other people, and 74.4% indicated that they did not write down a copy of their passwords in a notebook or diary. Keeping an electronic copy of passwords was also not a common practice, as 80% indicated that they did not do so.

The researchers also questioned the knowledge of the respondents concerning password cracking and theft. Many of the participants (80%) were aware of at least one technique used to steal or crack passwords. The most commonly indicated technique was a virus (36.85%). Respondents also indicated that worms (24.7%) and programme files (17.52%) can be used to steal passwords. A summary of the major findings in this survey are shown in Table 3.1

The researchers discussed and highlighted their most prominent issues in their findings. The respondents regularly reuse the same password, not only on all their different email accounts, but also many of them reuse these passwords on other applications on their computers. This finding, in conjunction with the fact that the majority of the respondents never change their passwords, creates a serious security risk for them.

The researchers indicate that the respondents display some knowledge of security awareness through the use of longer passwords. The average password length was 8.1 characters for the survey. Many of the respondents used passwords with eight characters or more.

Overall, the researchers have determined that the level of security awareness is still very low. The majority of the respondents are well-experienced with computer usage and have

had six or more years working with computers. The researchers indicate that a lack of security awareness training and inadequate training materials are the primary cause for low security awareness. Corporations and businesses should not assume their employees have a high level of understanding but should provide better strategies to equip their employees with these security skills.

Table 3.1: Summary of findings from University of Canberra survey

Significant Findings	Result	Percentage
Number of participants	884	-
Password length	Short (6 to 8 characters)	54.00%
Password reuse rate	High	56.10%
Password composition	Simple (alphanumerics only)	42.30%
Change passwords	Seldom or Never	61.90%

3.3 Wichita State University, USA, 2006

A survey was conducted on 315 participating students at Wichita State University, USA (Riley, 2006). The objective of the research was to identify what type of passwords the students were using. The researcher also wanted to assess the participants' knowledge about how they should be practicing secure password management compared how they were actually going about it.

The survey was composed of several sections of questions to determine the password usage habits and internet user account management. The questions were designed to determine the following:

- participant demographics;
- the number and types of internet accounts the participants have;
- password creation and storage methods; and
- participant attitude towards password management.

The overall findings from this survey indicate that the participants' password management habits are poor and insecure; these findings are summarised in Table 3.2. The general password characteristic results indicated that nearly 75% of the participants use a group of

predefined passwords, with 98% of them having three passwords in their group. Almost 60% of the participants did not change the complexity of these passwords even if the account was for a more sensitive website such as internet banking.

Over half of the respondents indicated that they *never* change their passwords on a system or website that does not require them to do so. The average length of time that the respondents were maintaining their primary password in use was thirty-one months. This means that the same password was maintained in use for over two years without being changed!

The password composition results showed that 85.7% of participants always use lower-case letters and 56.5% always use numbers when generating their passwords. 54.9% of participants use personally related words for passwords such as names of streets or pets. 49.8% apply the same method with particular numbers such as date of birth or telephone numbers. The use of meaningful or personally relating information is a common technique for ease of memorising passwords.

In the case of password reuse, 54.6% indicated they very frequently or always use the same password on different accounts. A variation on the same password was used on different accounts by 33% of respondents.

The survey results showed that 15% of the participants write down their passwords to remember them, while 28.6% use the browser's password storage facility to remember their passwords.

The difference between what the participants password practices were and the password practices they believed they should being using showed the following:

*73% believed they change their passwords every three to six months; however, over half of them never change them at all. * Just over half the participants believe their passwords should include special characters but only 5% of them actually do. * Nearly 64% believed that they should use seven or more characters in their passwords but only 35.5% indicated they use this many characters on a regular basis. * Nearly 70% of the participants indicated that use of personally related words and numbers is bad password management, yet even so, nearly 50% practice this anyway.

The research (Riley, 2006) concludes that the findings indicate that the respondents apply a simplistic and insecure approach to password management and generation. The respondents are aware of the recommended methods and practices surrounding password

management, yet the majority still do not implement these practices for themselves. The researcher also concludes that even in cases where password guidelines were available, the respondents would still use the least complicated and easiest to remember passwords.

The research finds that users are unaware of the true vulnerability of weak password management and the dangers that accompany this (Riley, 2006). The researcher recommends that further training around password vulnerability and security practices would help users to better understand security threats and subsequently improve their ability to protect against such threats.

Table 3.2: Summary of findings from Wichita State University survey

Significant Findings	Result	Percentage
Number of participants	315	-
Password reuse rate	High	54.60%
Password composition	Simple (lower-case letter) and (numbers)	85.70% and 56.50%
Use of personally meaningful information	High (commonly used to aid in memorising passwords)	54.90%
Change passwords	Seldom or Never	52.70%

3.4 Microsoft, Global, 2007

A large scale study was conducted on internet users by Microsoft (Florencio and Herley, 2007). The users were presented with an opt-in toolbar that would record and report on their internet website and password usage habits.

The installed toolbar was designed to monitor webpages that presented the participants with a username and password login screen. The toolbar would capture the details of the login information and report the details to a server hosted by Microsoft. The details of the logins were kept anonymous and private; none of the participants' user credentials were ever sent to Microsoft.

The information gathered includes the number of websites being visited and the number of passwords being used for logins. The toolbar reported on the bit-strength of the passwords being used per a website, the type of passwords that were being used by the participants and the frequency that passwords were forgotten and required resetting.

The results showed that the participants were following similar trends of poor password usage and lack of management. Data was collected from a total of 544,960 participants over a three month period.

3.4.1 Findings

The number of unique passwords being used by participants dwindled over time; users tended to start re-using the same passwords for different websites and would have an average of six different sites using the same password.

The bit-strength of the passwords was also low: users tended to reuse weaker passwords rather than stronger passwords. The participants would also primarily use weaker passwords (30 bits or less) on most websites unless the website would enforce the use of a stronger password (i.e. alphanumeric passwords with a longer character length). The analysis of password types being used was dominated by lower-case letter-only passwords. The number of password resets was recorded (for forgotten passwords) with a small sample of a certain websites. The researchers examined the number of users that accessed the Yahoo website, 2149 (4.28%) of the 50000 visitors had to reset their passwords over the three month period and that also constitutes 60% of the new users that registered in those three months.. The results indicated that the users were often visiting the password reset URL and requesting password resets. A summary of these predominant results are shown in Table 3.3.

The results of this research clearly show that password management is a problem for many internet users: users are unable to remember complex passwords and tend to favour weaker, simpler passwords. Participants are not using unique passwords for each website so the reuse password rate is high.

Table 3.3: Summary of findings from Microsoft survey

Significant Findings	Result
Number of participants	544960
Password length	Short (30 bits or less)
Password reuse rate	High
Password composition	Simple (lower-case letters-only)
Forgotten password rate	High

3.5 Malaysia Universities, Malaysia, 2007

A study conducted concerning password habits on university students in Malaysia (Tamil, Othman, Abidin, Idris, and Zakaria, 2007) showed that the majority of students were not adhering to secure password usage habits and practices. The research, conducted using a survey method, was disseminated to random students at a few different universities in Malaysia. The survey was comprised of two sections of questions. The total number of students surveyed was 194.

The first section of questions was designed to gather general demographics about the participants, including age, gender, level of education and field of study. The second section of questions was composed of question relating to the participants' computer accounts and the methods used by the participants to manage their passwords for these accounts.

The results of the survey provide strong evidence that many of the users were not practicing secure password management. While many of the users had only a few accounts to manage, they would often reuse the same password for these different accounts.

A summary of the most significant results from this survey are shown in Table 3.4 The majority were able to memorise their passwords; however, they were using passwords of eight character or less. The bulk of the participants had five or fewer unique passwords they were using. The majority of participants either never changed their passwords or weren't aware that they should be doing so.

The participants are regularly reusing the same password on different accounts (85.90%). Of the participants who indicated that they do reuse passwords, nearly half of them (46.40%) reuse the same password on all of their user accounts. Nearly 60% of the participants used either letter-only or number-only derived passwords. The combination of short passwords with limited character sets make these passwords weak and simpler to crack with brute-force attacks.

3.6 University of Auckland, New Zealand, 2009

Researchers at the University of Auckland in New Zealand (Notoatmodjo and Thomborson, 2009) conducted a research survey to gauge users' perceptions of password security

Table 3.4: Summary of findings from Malaysia Universities survey

Significant Findings	Primary Result	Percentage
Number of participants	194	-
Password length	Short (8 characters or less)	60.00%
Password reuse rate	High	86.50%
Password composition	Simple (letters-only or numbers only)	57.30%
Change passwords	Seldom or Never	85.90%

and how they manage their passwords based on that security understanding. The researchers hypothesised that users will allocate a level of importance to different user accounts and that they will create a password for that account based on this level of importance. Password length and complexity will increase based on this level of security importance.

The researchers conducted a survey with 26 university students as the participants. The participants were asked to complete the research in two parts. The first part consisted of general demographic questions about the participants, including their field of study, how long they had attended the university and their amount of experience with computers.

The second part of the research required participants to complete the task of listing all of their user accounts and passwords. They had to group their passwords based on perceived similarities of security.The researchers wanted to determine how the participants organise and select their passwords, and asked the participants to explain the reasoning for the grouping and for how they assessed the importance of each account. The participants assigned numbers to the accounts and passwords. These numbers were used in the statistical analysis by the researchers and allowed for privacy preservation of the participants' user account information.

The participants then needed to calculate the number of characters in each password, and rate both their perceived security level and the difficulty of remembering their passwords. Finally, the participants had to collate the password and group information into columns based on the value of the user account and how often they used each account, assign the password code to the account, specify if the password had been reused and provide the reason why the password had or had not been reused.

The study's results indicated that there was no correlation between the participants' perception of security importance and the length of their passwords; neither was there a correlation between the password length and the difficulty of password recollection. The

participants' results showed there was, however, a correlation between the perception of security importance and the difficulty of recalling the passwords.

The researchers showed that the number of online user accounts would increase as participants increased their internet experience. This was also confirmed in the research conducted by Gaw and Felten (2006).

The survey results indicated that reuse of the same password on different accounts would increase as the participants created more online user accounts.

The researchers queried the participants as to why or why not they would reuse a password on a different account. The participants were presented with a number of statements to select for their answer. The results did not highlight one specific reason as to why the participants did not reuse passwords. The highest ranked answer with 28.4% was that participants believed the account was too important to have the same password as any other. 35.1% of the participants who indicated that they did reuse passwords on different accounts cited their reason as because it was easier to recall their passwords.

The researchers analysed the account and passwords group to determine how the participants formed their groups. The researchers decided on five subjective groups: Type of Service, Risk, Frequency, Alias and Sharing. The largest group, Type of Service, constituted 72% of the accounts and was the type of usage the participants had for the account (i.e. educational or financial). The next category, Risk (18.6%), were for accounts that had information that was more important and needed to be more secure than other accounts. The Frequency category accounted for 5.2% and contained accounts that were regularly used and logged into. The Alias category was accounts that were based on the login user name, or alias; this accounted for 2.5%. The final category, Sharing (1.7%), contained account credentials that the participants shared with other people. These categories were used by the participants to assign the necessarily perceived security level passwords.

The researchers also calculated the total number of high and low importance account groups based on the rankings that were collected from the participants. They determined that there were 37 high importance account groups and 93 low importance accounts.

The researchers then determined the password reuse statistics from the number of accounts in the account groups. There were a total of 68 accounts in the high importance account group, 63% of which had not had their password reused. In the low importance group, there were 253 accounts and only 18% did not have their passwords reused on another

account. 50% of all the participants had reused a password at least once on another account.

The survey results indicated that the participants had fewer reused passwords on their high importance accounts than on their low importance accounts. The high importance account passwords are considered to be of a higher perceived level of security and more difficult to remember.

The researchers concluded their paper with a summary of their findings. The researchers do acknowledge that their sample size was quite small and entirely composed of students. The results of the study showed that the participants created groups for their user accounts and assigned different level of importance and security to them. These more important accounts were assigned more complex and longer passwords. These account passwords are seldom shared with other accounts.

Table 3.5: Summary of findings from University of Auckland survey

Significant Findings	Result	Percentage
Number of participants	26	-
Password length	Short (average length of 5 characters)	54.00%
Password reuse rate	High	56.10%
Password composition	Simple (numerics only)	62.60%
Change passwords	Seldom or Never	61.90%

3.7 Pontifical Catholic University of Rio Grande do Sul, Brazil, 2012

Researchers at Pontifical Catholic University of Rio Grande do Sul in Brazil conducted a research survey on the password habits and the memory limitation of people (Pilar, Jaeger, Gomes, and Stein, 2012). The researchers wanted to determine whether age and/or educational background would have an effect on the way users remembered and stored their account passwords. The results of the research were not what the researchers expected.

The researchers conducted a survey with 263 participants. There were three age groups surveyed: 18 to 39, 40 to 64, and 65 to 93. These participant groups were then further divided according to their educational backgrounds: those who had not completed high

school, those who had completed high school but not attended a college, and those who had completed at least some college education.

The researchers interviewed the participants and presented them with questions relating to password length and composition. 62.6% of participants used numerics only in their passwords; 24.3% used only alphabetics; and 12.4% used alphanumeric passwords. The majority of the passwords (70%) were created by the users while the remaining 30% were created by the system or application they were using.

The researchers analysed the results from the survey to determine the number of password uses and number of unique passwords each participant had. The results indicated that the average number of uses for passwords per participant was 5.38 and the average number of unique passwords per participant was 3.98. The researchers pointed out that the number password accounts uses increased as the level of education increased, as did the number of unique passwords. The age factor did not affect either of these results.

The researchers next examined whether age or education level would affect the number of characters the participants used in their passwords. The average password length for the participants was 4.89 characters. The results indicated that the younger age group had the highest number of characters, followed by the middle and then the oldest group. The results also showed that the higher level education group also used more characters in their passwords than the education level below them.

The final section of questions in the survey related to difficulties the participants encountered with remembering passwords. The researchers determined that 72% of the participants had problems remembering their passwords. The highest percentage came from participants under the age of 64 that had completed high school. Another set of participants with a high number of password recollection difficulties were the participants with college level education, regardless of their age.

The results about memory difficulties and number of passwords were then correlated. Overall, findings showed that regardless of education level or age, the most significant factor affecting the participants' abilities to remember passwords was the number of passwords and the number of unique passwords.

The dataset for questions relating to password reset requests and keeping written copy of password showed that 59.8% of participants that had problems remembering their password kept a physical copy of it. Only 44.6% of participants that did not have password recollection problem kept a copy of the password written down. These findings support

the results that more passwords and unique passwords lead to higher password memory problems.

The researchers also queried the participants about the need to have their passwords reset. Again, the majority (67.9%) of participants with password memory difficulties reported having had their password reset at least once, while of the participants without memory difficulties, only 21.6% needed to have their password reset.

The researchers' discussion about their findings showed that their initial hypothesis that age and/or educational background would affect the participants' abilities to remember their passwords was incorrect. The results showed that as the number of passwords and unique passwords increases, the participants' abilities to remember their passwords decreased. The key findings of this study are summarised in Table 3.6

Table 3.6: Summary of findings from Pontifical Catholic University of Rio Grande do Sul survey

Significant Findings	Result	Percentage
Number of participants	263	-
Password length	Short (average length of 4.89 characters)	-
Password reset rate	High	67.90%
Password composition	Simple (numerics only)	67.60%
Password recollection	Difficulties remembering passwords	72.00%

3.8 Summary

The results from these studies have produced similar findings about the password management habits of users from different countries and continents. Users exhibit generally poor password management practices; this does not seem to have a specific connection to any demographic category such as age, gender or educational background.

The participants of the surveys demonstrate that having to manage large numbers of user accounts affects their ability to use strong passwords and leads to bad habits such as regularly reusing the same password on multiple user accounts. The research papers suggest that users are creating passwords with an inadequate number of characters and character types limited in complexity.

The studies have also demonstrated that users' perception about the security of their passwords would vary depending on importance of their user account. The findings also

indicate that training on password management and security awareness is *not* being regularly provided.

This research paper utilises the data collation methods from the previously related research into password management to study the behaviour of South African internet and computer users. The method and tools used in this research are detailed in the following chapter.

Chapter 4

Data Collection

4.1 Introduction

The study was conducted as the core of this research to gain insight into attitudes and behaviours of computer users with regard to their usage and management of passwords. The study will cover both the personal and professional habits of the participants' password usage.

The research method is designed to gain predominantly quantitive results, with fewer qualitative results providing slightly more depth into the participants' opinions on the subject of password usage and management.

The details of the research design will follow in section 4.2 and provide detailed information regarding the data collection process, the analysis of the data and the limitations of the selected research design. A description of the data collection tools and distribution methods used in this research are detailed in section 4.3. The research was conducted using an online survey and distributed through the use of online communications services. The survey response results and the analysis of the response results are in section 4.3.3 and section 4.3.4 respectively.

The remainder of this chapter includes section 4.4 which details the limitations of this research methodology. Section 4.5 explains the required ethical considerations for survey-based research.

4.2 Research Design

A survey-based research design was selected as the data collection technique for this study because it would provide the best method for gathering information from computer users about their experience with password management. The survey was designed to elicit selected information from the respondents regarding their attitudes, opinions and habits around password usage and management, both within their organisation/institution and in their personal capacity. The questions posed to the participants can be found in Appendix A. The questions from the survey were designed to meet the previously mentioned objectives of this research in section 1.4.

An online survey platform was selected due to the ease of accessibility for participants and ability for distributing the website link via a number of online services such as social networks and email. The online survey allowed the research to be advertised and accessed by a broader and more diverse group of participants. However, the use of an online survey tool posed a challenge to the South African only context of the research, as any online user would be able to access it. The survey did, however, state in the disclaimer that it was for South African residents only and by accepting the disclaimer a respondent agreed to the term and conditions Appendix A. There is, however, no way of verifying this. The participants were also asked which South African province they resided in the demographic questions section, this however did not guarantee that only South African residents will participate.

The survey consisted of predominantly closed-ended questions, as these provide more quantitive results and also allow the participant to complete the survey in a timely fashion. The statistics for the survey times are provided in the analysis section (section 4.3.4). There were fewer open-ended questions presented to the participants. These open-ended questions allowed the participant to provide optional answers to the questions and thereby present their opinion or attitude about a particular question. A full list of questions posed can be found in Appendix A.

The survey questions were divided into four sections. The first section gathered demographic information about the participant, including each participant's age group, gender, employment status and industry, income bracket and internet usage behaviour. The second section of questions enquired about each participant's user account and password behaviour within a professional capacity. The third section posed questions pertaining each participant's personal habits surrounding user account and password behaviour. The

fourth and final section contained ranking questions, whereby the participants would order the answers to the question as per their own security perception.

The process of development and formulation of the questions to be posed commenced with reviewing past survey studies as discussed in Chapter 3. Upon reviewing the questions that were included in previous surveys, the researcher contacted one of the primary authors of a specific paper Tamil *et al.* (2007) and asked for permission to reuse some of the questions in the paper for the researcher's survey. An email granting permission was sent by the author; acknowledgement has been made to the author of this study.

The research technique did include the collection of sensitive information from the participant in terms of password habits. However complete anonymity was observed by the exclusion of personally identifiable information as part of the survey and the storage of the information in secure electronic format[1].

The survey was limited to English-only as the language choice. According to the 2011 Census by Statistics South Africa (Lehohla, 2012), English is the fourth most frequently spoken language with 9.6% of the population identifying English as their first language. The fact the survey is in English may have prevented certain population groups from participating in the survey. English is also the primary language of businesses and tertiary educations institutions in South Africa.

The selection of an online survey would most certainly exclude groups within the population that did not have access to a computer and/or the internet. While this will reduce the size of the sample group and representation of the population, the study is focused on gathering data from a population who are users of computers and the internet, both in a personal and professional capacity.

4.3 Research Instruments

The research instrument selected for this study was an online survey. An online survey enabled the researcher to distribute the survey invitation using online communications services and enabled the results to be collected and stored in an online computer application. The usage of an online survey also eliminated the need to manually deliver and collect survey questions and responses.

[1] http://www.limeservice.com/en/how-it-works/21-english/general-content/39-data-protection-statement

4.3.1 Survey Software

There were a number of online survey platforms reviewed for use in the research design. These included Survey Monkey[2], Survey Gizmo[3] and Google Forms[4]. The chosen online survey application was Lime Survey[5] which was implemented using the hosted commercial service Lime Service[6].

Lime Survey was selected for a number reasons. Lime survey is popular and widely adopted tool for online surveys. The Lime Survey publishes a list of government and commercial companies[7] that have used the software. There is also a list of education institutes[8] that have encorporated Lime Survey as part of their survey toolset.

Lime Survey offers a hosted, commercial solution on the Lime Service website. Lime Service proved to be a minimal cost solution and also enabled the timely creation and deployment of live surveys. Lime Service also provides professional support services to assist in the creation of surveys and to handle technical support requests.

Additionally, Lime Service offers reliable and secure management of the data collected in the survey. The Data Protection Statement[9] on the website iterates the commitment of the service to not publicly disclose any of the collected data, to track the users with cookies and to prevent third-parties from accessing the information.

Online surveys present another challenge in trying to prevent participants from repeating the survey. Lime Service provides a cookie based[10] feature that prevents a participant from completing the survey more than once. Lime Service will detect that the participant has a completed cookie installed on their computer and notify them that they have already completed the survey. This feature was enabled for the survey conducted in this research but does limit the use of a shared computer which is typically found in a "home" environment.

[2]http://www.surveymonkey.com
[3]http://www.surveygizmo.com
[4]https://docs.google.com
[5]http://www.limesurvey.org
[6]https://www.limeservice.com/en
[7]http://www.limesurvey.org/en/about-limesurvey/references
[8]http://www.limesurvey.org/en/component/content/article/1-general-news/193-ask-limesurvey-which-universities-are-using-limesurvey
[9]https://www.limeservice.com/en/component/content/article?id=39
[10]http://manual.limesurvey.org/wiki/Creating_a_new_survey#Publication_.26_access_control

4.3.2 Survey Distribution

The target representative population for this survey that has been described in section 4.2 would require both computer and internet access in order to participate in the survey. The distribution method selected was to use online media such as social networking and email. As such, it was determined that using these forms of media would prove to be the most effective means of distributing the survey. Individuals who were using social media websites and email were most certainly familiar with managing usernames and passwords.

The online median selected was social networking websites. The researcher had access to both Facebook[11] and LinkedIn[12], two of the most popular social network websites on the internet. The description of the survey was intentionally kept short and to the point, stating the nature of the survey, the privacy protection and targeted participants.

A brief description and link to the survey were initially posted on both of these social media platforms on the 25th of March 2013, requesting the researcher's contacts to participate in and forward the survey to their contacts as well. The survey posting was repeated on a regular basis in order to continue encouraging the contact to participate in the survey. By incorporating the use of social media as a distribution mechanism, the author anticipated being able to leverage the viral nature of social media sites and rely on participants to forward the online survey link to their contacts.

The researcher also utilised email contact lists to advertise the survey. An email was drafted with the same description and link, as with social media websites, to the survey website. The email invitations also requested the recipients to forward the request on to their own contacts and encourage them to take part in the survey. Likewise, the email requests were repeated on a regular basis, starting from the 25th of March 2013. The requests were sent out over a period of eight weeks.

The researcher contacted the Rhodes University Computer Science Department to request that the survey link be distributed to the students enrolled in its undergraduate courses. The request was accepted and the email was sent out to over 500 students in various faculties. These emails were sent out on the 14th May 2013 and 15th May 2013. The survey was closed on the 20th of May 2013, after eight weeks.

The number of responses by dates during the period the survey was conducted is shown in Figure 4.1. The researcher sent out regular reminders to continually encourage contacts

[11] https://www.facebook.com
[12] https://www.linkedin.com

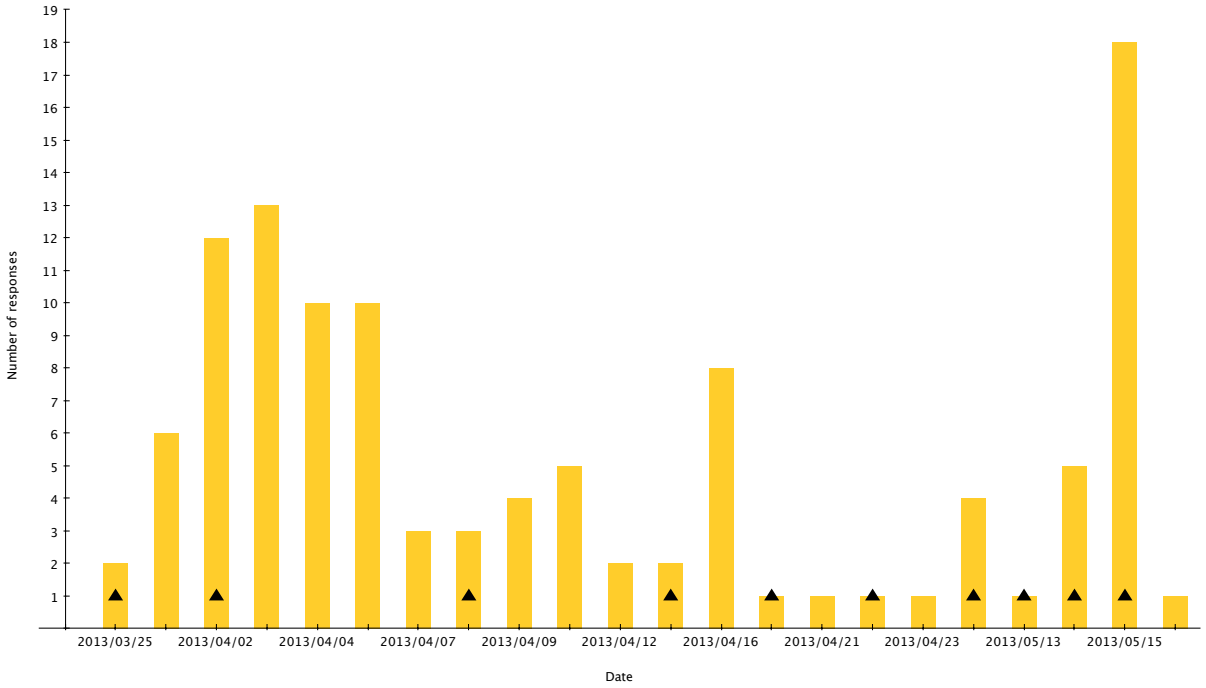

Figure 4.1: Responses over the survey period time

to participate and forward the survey link to others. The days on which a reminder was posted or emailed are indicated on Figure 4.1 by the triangle symbol.

4.3.3 Response

The survey questions were formulated for participants who are part of an institute or organisation that has implemented a security policy for user accounts and passwords. The survey requests were distributed to professionals employed in a number of industries and students attending tertiary institutions.

A summary of the response results is shown in Table 4.1. There were 163 responses collected, of which 117 were fully completed. The population sample collected includes both professionally employed and student participants; as such, a completion rate of 71 (78%) was obtained. The details of the data collected will be expounded upon and explained in the following chapter.

The 46 incomplete responses contained either partially or totally incomplete responses. There were 16 empty responses with no questions answered at all. The remaining 30 participants had varying degrees of completion. There were 4 participants who completed

the final question; however, they did not complete the previous ranking questions in that section (Appendix A. [Questions 56 to 58]).

Table 4.1: Survey Response Summary

Response Summary	Number of responses
Total number of responses	163
Fully completed responses	117
Total incomplete responses	46
Partially incomplete responses	30
Empty responses	16

The respondents who only partially completed the survey were either unable to understand or complete some of the questions and/or interrupted their survey session and did not return to complete it at a later stage. These results were excluded from the analysis of the data and did not form part of the findings of this study.

4.3.4 Analysis

Lime Service software is equipped with a 'statistics of responses' toolset. The software provides the ability to run statistical counts on all the collected dataset, whether completed or not. The statistics tools provide a count, percentage and graphs for all questions. The survey owner has the ability to select and filter specified question groups, questions, or answer fields, thereby creating pivots to determine results from a specific set of variables.

The Lime Service software also allows the user to select multiple answer fields, enabling the results of comparative and/or correlated results to be determined from the survey results. The results from the survey were also exported into Microsoft Excel where data was analysed and summarised using the pivot table feature. However, the analysis of the survey data was primarily done using the statistics tool provided by the Lime Services website.

All survey statistic results (including the filters) can be exported to other data formats comma-separated values, R-data and SPSS. There were several other software programs reviewed, including IBM SPSS Software[13], GNU PSPP[14], RStudio[15] and SOFA[16]. However

[13]http://www–01.ibm.com/software/za/analytics/spss
[14]http://www.gnu.org/software/pspp
[15]http://www.rstudio.com
[16]http://www.sofastatistics.com/home.php

none of these tools were selected due to either financial costs, over complexity and/or the inability to correctly import the survey data.

4.4 Limitations

The survey methodology can be affected by several limitations. As per the weakness mentioned on the fundamentals of survey research (Glasow, 2005), a dearth of responses, participants misreporting or by misbehavior, and participants' failure to correct their own behaviour and attitudes may affect the results of the survey.

The use of an online survey has its own limitations. As mentioned in section 4.2, the language selection and necessity for computer and/or internet access will have limited the sample of population that may participate in the survey. The distribution of the survey through the usage of the social media and email will also have had an added effect on the people participating in the survey. First-level contacts of the researcher may have had common demographics, whether these were age, profession, industry and/or gender; these may have influenced or biased a particular participant group.

4.5 Ethical Considerations

Rhodes University requires all researchers to adhere to the Ethical Guidelines for Human Subject[17] testing. In order to comply with these guidelines, the researcher must complete the Ethical Standard:Research Protocol document[18] for approval.

This document was completed by the researcher and approval was confirmed by Rhodes University. While there is a possibility of harm from the research being conducted, all acceptable measures were taken to minimise the likelihood of its occurrence.

[17] http://www.ru.ac.za/media/rhodesuniversity/content/research/documents/Ethical_Guidelines_Human_Subjects.pdf

[18] http://www.ru.ac.za/media/rhodesuniversity/content/research/documents/Human,Ethics,,Approval,Application,Form.doc,-,03,,March,2009.doc

4.6 Summary

This chapter has covered the researcher's approach to the data collection, analysis and verification process. The researcher determined that a survey-based methodology would be the best suited method to gather and assess the participants' attitudes and behaviour toward password and user account management.

The strengths and weakness of design, instruments and analysis have been covered in this chapter, as well as the limitation of the survey-based research. The ethical requirements of such research were reviewed and adhered to during the research design process.

The following chapter investigates and analyses the results from the online survey. The results from the users' responses provide insight into the participants' password management habits, their perceived security awareness and the technologies they use to maintain their password security.

Chapter 5

Analysis

5.1 Introduction

The researcher investigated and reviewed the statistics from the responses in the survey results. The analysis section of this paper intends to present information about the participants in regard to their demography, password usage habits, their perceptions on security and their use of additional security technologies.

The detailed analysis of this chapter will begin with the demographic details of the participants from the survey in section 5.2. In section 5.3 the participants' perceptions towards password authentication and their own password security habits are investigated.

The analysis of the participants' password management habits, in both professional and personal contexts, are detailed in section 5.4 and section 5.5. In the section that follows, the researcher investigates specific habits and attributes of password management exhibited by the survey participants which include password reuse (section 5.6), password length (section 5.7) and password complexity (section 5.8).

The use of password management software and multi-factor authentication are analysed in section 5.9 and section 5.10 respectively. These sections investigate the usage and effect these security technologies have on the participants' password management.

The final section details participants' perceptions and exposure to security awareness training (section 5.11). This section details the amount of training the participants have had concerning information security and, more specifically, password security.

Unless otherwise specified, percentages are calculated based on the 117 completed surveys as discussed in section 4.3.3.

5.2 Demographics

This section provides analyses of the characteristics of the participants from the survey data. The demographic questions included information relating to the age, gender, employment status, industry of employment (or study) and internet usage of the participants. These survey questions (Question 1 to 13), are available in Appendix A.

5.2.1 Findings

The demographic questions group in the questionnaire show that majority of participants (65.81%) were between the ages of 26 and 45. This majority of respondents was divided amongst two age groups: 26 to 35 years (36.75%) and 36 to 45 years (29.06%). The other notable age group was 19 to 25 years (22.22%). In terms of gender, 59.97% were male respondents.

Table 5.1: Industries of employment or study of the respondents N=117

Industry	Count	Percentage
Information Technology	58	49.57%
Academic/Education	11	9.40%
Banking/Investment and Finance	10	8.55%
Other	8	6.84%
Sales and Marketing	7	5.98%
Engineering	4	3.42%
Hospitality	3	2.56%
Safety and Security	3	2.56%
Government	2	1.71%
Health & Fitness	2	1.71%
Retail	2	1.71%
Insurance	2	1.71%
Legal	2	1.71%
Human Resources	1	0.85%
Manufacturing	1	0.85
Telecommunications	1	0.85%

The employment status and industry questions showed that nearly 65% of the respondents were currently employed, 20.51% were students and 11.97% were currently self-employed.

The largest group of participants (49.57%) were from the Information Technology (IT) sector; however, the remaining respondents were quite diverse in their current industry of employment or study, as seen in the Table 5.1.

In terms of internet usage and online service usage, all of the respondents had at least one e-mail account and only three of the 117 claim to not have any social networking accounts. Over 90% of respondents have Facebook accounts and nearly 60% have Twitter accounts. The respondents also use a number of other online services and resources. Nearly 65% of the respondents use e-commerce websites for purchasing online products and services, 47% use online auctions and classifieds websites, and 29% play games online.

5.2.2 Analysis

The analysis of the demographic statistics from the survey show that the significant majority of participants are between the ages of 26 and 46. Most of this group of respondents are either employed or self-employed, with nearly half of them in the Information Technology industry. Most of the group use a number of internet services and resources including social networking, email and e-commerce websites.

The dataset indicates a significant group of respondents between the ages of 19 and 25. This group of respondents is almost entirely composed of students or part-time employed people. 16 of these 26 respondents are studying towards accreditation in the Information Technology sector. The overwhelming majority of these participants are online internet users of such services as Gmail, Facebook, Twitter and online gaming services.

The remaining minority of respondents (11.96%) were over the age of 46 and were all either employed or self-employed. The majority were distributed between Information Technology and Academia. Most of these respondents are users of the online services such as Facebook and Gmail. The majority of these users also used e-commerce websites such as Kalahari and/or Amazon.

5.2.3 Review of analysis

The results of the survey demographics show that the majority of the respondents are users of a number of internet services such as social networking, email, online gaming and e-commerce websites. All of these online resources are extremely popular and require the

participants to manage account credentials (in most cases username and passwords) to maintain their security and privacy. As shown in Table 5.2, many of the participants use a variety of online services.

Table 5.2: Participants using online services N=117

Online Service	Count	Percentage
Facebook	106	90.60%
Gmail	104	88.89%
LinkedIn	77	8.55%
E-commerce Websites (Kalahari, Amazon etc)	76	64.96%
Youtube	72	61.54%
Twitter	70	59.83%
Google Plus	58	49.57%
Online Auction/Classifieds websites	55	47.01%

The respondents are made up of mostly students (20.51%) and currently employed people (64.96%). The student respondents are mostly under the age of 25, while the employed respondents are predominantly between the ages of 26 and 46. The student group has grown up in an era defined by technology and computers. The older group, on the contrary, grew up with much less exposure to computers and almost certainly very little or no online internet experience.

Usernames and passwords are the primary access control mechanism deployed in academic institutions and businesses (Ives *et al.*, 2004) (Furnell *et al.*, 2000). The respondents that use the computer facilities at these institutions and organisations will need to manage a number of usernames and passwords in order to continue having access to digital information and resources.

The respondents will also need to manage the username and passwords to their private internet services in conjunction with their employment or student credentials. The manner of how they manage each of these sets of credentials will be detailed in the sections that follow.

5.3 Online behaviour and perceived security posture

The participants of the survey were presented with a number of questions regarding their opinions about the need for credential enforcement policies and whether or not they

believed their own user accounts and password management practices were secure enough. (See Appendix A (Questions 13, 31,32,55 and 60))

5.3.1 Findings

The overwhelming majority were divided approximately in half in terms of level of concern towards their online user accounts and the extent to which they ensure that their credentials remain safe and secure, with 45.3% stating that they have genuine concerns about the security of their accounts and protecting them to the best of their ability. The other half of the respondents, comprising 44.44%, indicated an extreme consciousness towards the security of their account credentials and trying to employ their utmost protection for them.

Many organisations employ password policies that enforce the best practices of password management (Wood and Shield, 2008). These password policies include, among others, the regular changing of passwords, minimum number of characters and the use of different types of characters. The respondents were questioned as to whether or not they felt it necessary for their organisations or institutions to institute these controls. The overwhelming majority (93.16%) agreed that it was necessary to implement these measures. The remaining 6.84% that did not think it was prudent to implement password policies responded with statements such as 'remembering complicated passwords is difficult', or 'changing passwords on a regular basis is annoying', or that 'it would just be simpler to use the same password on all accounts'.

The questions about the strength and secureness of their personal accounts' passwords again demonstrated that the majority of respondents (86.32%) were confident that their personal passwords were strong and secure.

There are a number of other access control technologies that can be used in conjunction with usernames and passwords (Bhargav-Spantzel, Squicciarini, Modi, Young, Bertino, and Elliott, 2007) (O'Gorman, 2003). These other access control technologies include, among others, security tokens, one-time passwords and biometrics. The respondents were asked whether or not usernames and passwords were sufficient protection for their user accounts. The results were divided very closely with 52.14% indicating that usernames and passwords alone were not adequate enough protection for their user accounts.

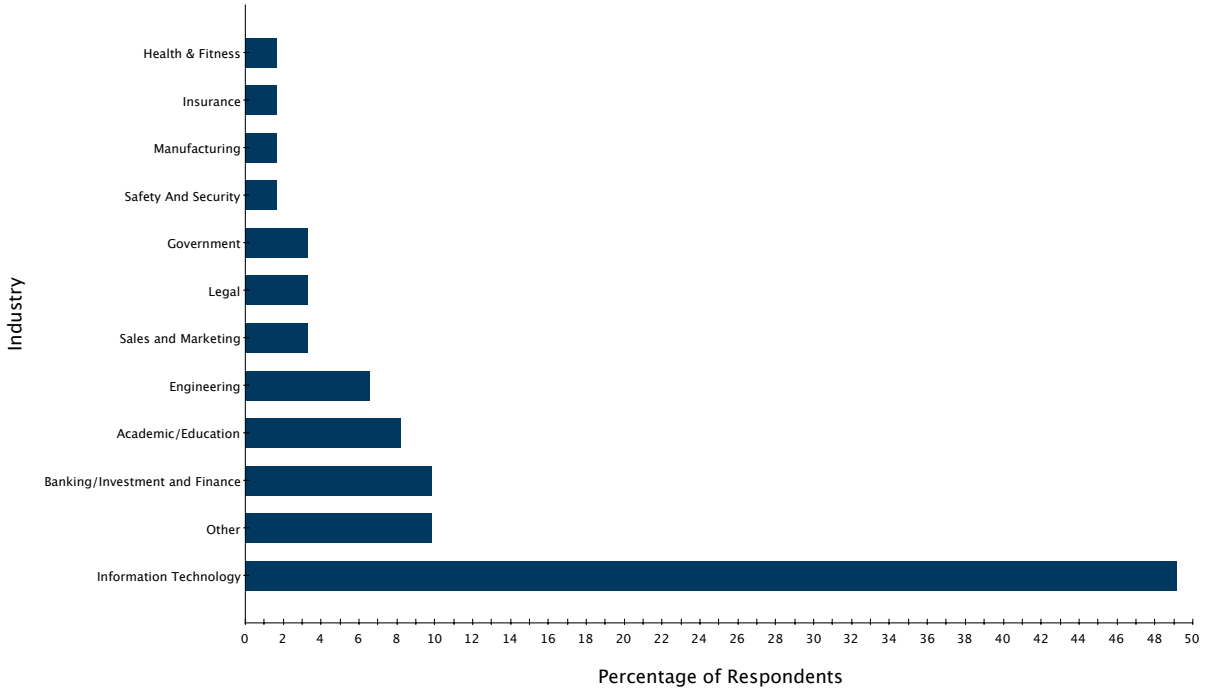

Figure 5.1: Industries of respondents indicating passwords are not enough security

5.3.2 Analysis

The preponderance of respondents are aware of the necessity of securing and protecting their user account credentials. These opinions range from being consciously concerned to extremely concerned about the protection of their usernames and passwords. These concerns are expressed both in a personal capacity as well as in work and study environments.

The use of password policies in the organisations and/or institutions was acknowledged and supported by the majority of the respondents. The use of password policies has become common amongst most organisations and institutions. Many internet websites also employ password policies, and while they may not be as stringent as organisational policies, they still force the user to create seemingly more complex and hence more secure passwords for their accounts.

Opinions on the effectiveness of password authentication were split, with 52.14% indicating that passwords were not enough protection for their authentication processes. Username and passwords have been the primary access control technology for a number of years; however, the theft and cracking of passwords has become a relatively trivial task in recent years (Marechal, 2008). There are a number of other access control technologies that can be implemented to augment the strength and security of users' credentials.

Those respondents who indicated that usernames and passwords were not adequate enough protection for access control, were comprised of nearly 50% of people in the Information Security industry. The 61 respondents who expressed the need for an additional access control mechanism are represented in Figure 5.1.

5.3.3 Review of analysis

The fundamental need to protect and secure credentials is well understood by the majority of the respondents. These fundamentals are enforced in the organisations and institutions in which the respondents are users of computer resources and networks. The respondents are mostly in support of these policies and are of the opinion that these password policies improve the security and integrity of their user credentials.

The respondents, however, are not in agreement as to whether or not usernames and passwords are adequate protection for access control. The respondents were almost divided in two with their opinions. The majority of the respondents who indicated that usernames and passwords were not adequate enough protection were employed in the Information Technology sector. The recommendation to implement additional security measures and technologies into access control processes has been supported and advised by the Information Security industry for quite some time (Khandelwal, 2012) (Siciliano, 2012).

The respondents are mindful of the security needs around usernames and passwords. They are obliged to maintain a certain level of security in the work or study place due to the implementation of password policies. The respondents also feel that they are protecting their user credentials. A portion of the respondents also feel that these user credentials are suitable enough protection for their network and computer accounts. In the next sections, the researcher analysed whether these beliefs are substantiated or not.

5.4 Organisation password management and policies

Corporation and academic institutions are encouraged to implement password policies and training to guide their users on good password practices (Granger, 2002).These password policies should address elements such as password length, complexity, expiration and

reuse. The respondents were presented with questions relating to the use of password policies in their organisations and/or institutions. The survey questions (Questions 14 to 32), for this section are available in Appendix A.

The majority of respondents were accustomed to the use of a password policy within their business or academic institution. This majority accounted for 84.62% of the respondents.

5.4.1 Password length

Password policies can consist of a number of controls, controls which can include password length, password complexity, expiration of passwords and password history tracking. Some organisations may also implement additional security technologies to improve and complement the user access control process.

84.85% of the respondents are required to have a minimum number of characters for their passwords. The respondents were questioned as to the number of characters they are required to use when selecting their passwords. The vast majority (76.74%) are required to use between five and eight characters for their passwords. The results also indicate that 15.12% of respondents are required to use between nine and twelve characters, 3.49% are required to use between twelve and fifteen characters and 2.33% are required to use between one and four characters. None of the respondents is required to use more than fifteen characters for their passwords. These results for the number of characters required are shown in Figure 5.2.

5.4.2 Password expiration

The bulk of respondents are required to change their passwords on a regular basis. The results of the survey reveal that 81.82% are forced to change their passwords periodically. For the most part, the respondents are required to change their passwords every thirty days. This time period constitutes for 58.33%, while 16.67% are required to change passwords every sixty days. 10.71% have mixed response time periods, including every three months, six months, yearly and each term or semester. 9.52% of respondents are required to change their passwords every ninety days. These findings are represented in Table 5.3

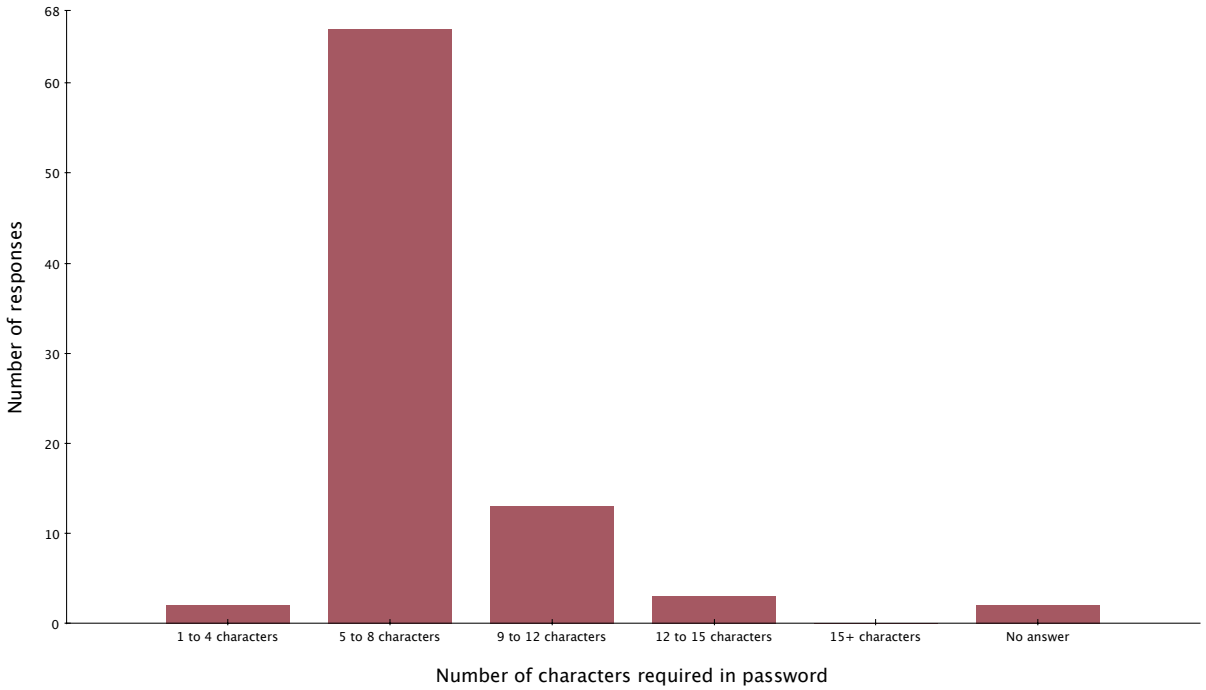

Figure 5.2: The number of characters required for passwords per number of respondents

Table 5.3: Organisation password change frequency N=81

Time period	Count	Percentage
Every 30 Days	49	58.33%
Every 60 Days	14	16.67%
Other/Mixed	9	10.71%
Every 90 Days	8	9.52%
Bi-weekly	1	1.19%

5.4.3 Password complexity

Password complexity can affect the strength of the password that is being used. The majority (78.79%) of the respondents are obligated to use both alphabetical and numerical characters in their passwords. 67.68% are, however, not prevented from using names or dictionary words for their passwords.

5.4.4 Password history and tracking

Password policies that implement password history tracking are intended to prevent system users from re-using the same passwords for a specified number of password change cycles. The majority, represented by 51.52% of respondents, indicated that they are subject to password history tracking and prevention. 26.26% indicated that they were not subject to this control, while 22.22% did not give an answer for this question.

5.4.5 Number of user accounts and password reuse

Computer users may have a number of user accounts and passwords to remember in order to gain access to a company's or institution's digital information. The result from the respondents indicated that 82.05% have one to five user accounts, 11.97% have six to ten user accounts, 4.27% have fifteen or more user accounts and 1.71% have eleven to fifteen user accounts to access the computer resources. The bulk of the respondents (67.52%) indicated that they reuse the same password on different accounts within their organisation.

5.4.6 Password recollection

A common issue for users is the need to remember and manage all of the usernames and passwords for their access controlled application. The respondents were questioned about the techniques they use to remember and manage their user credentials. 37.61% indicated that they reuse the same or similar password on all their accounts; 35.90% indicated that they memorise all of their passwords; 13.68% use a password management software tool; and the remaining 12.82% write their passwords down or keep them in a spreadsheet. These results are displayed in Figure 5.3.

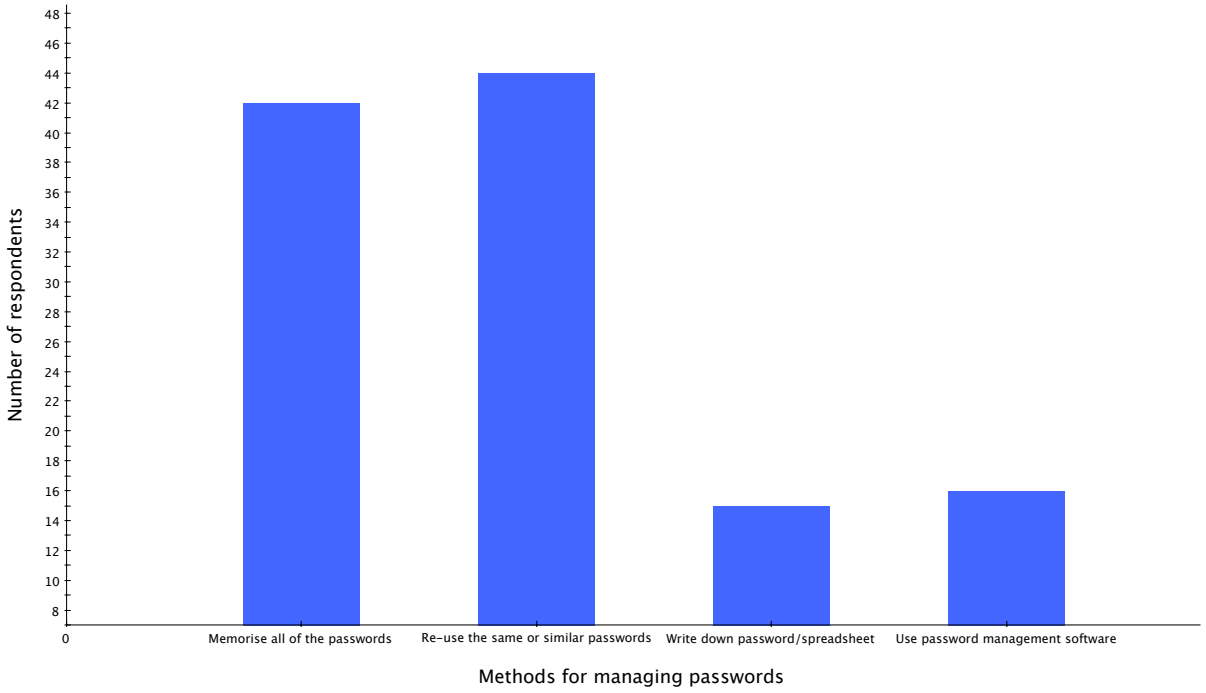

Figure 5.3: Methods for managing and remember passwords

5.4.7 Password disclosure

Organisations would disapprove of their users disclosing passwords to other users in their networks. Respondents were questioned about whether or not they shared their passwords with other people in their organisation and whether or not they knew other colleagues' passwords. The survey results indicated that 32.48% of participants had shared their password with someone in their organisation.

The results also indicate that 39.32% knew the passwords of other computer users within their organisation. An analysis of the correlation between participants sharing passwords and knowing someone else's passwords showed that 63.16% of those sharing their password also knew somebody else's password.

5.4.8 Multi-factor authentication

Respondents were questioned as to whether they use multi-factor authentication in their organisation. 64.96% responded that they did not use additional verification technology and 19.66% did not answer the question. The remaining 15.38% responded that they did use multi-factor authentication. Further analysis on multi-factor authentication is described in section 5.10.

5.4.9 Security awareness training

Security awareness training is used by organisations to educate their computer users in best practices and methods of secure computer resource usage. The survey results show that nearly 60% of respondents' organisations do not provide security awareness. 24.79% of the organisations do provide security awareness training and 15.38% of respondents did not provide an answer.

5.4.10 Analysis

The greater part of the respondents has been exposed to an information technology environment that has a password policy implemented and necessary controls in place. The respondents have been exposed to the controls that are most commonly implemented in a password policy.

Password management and multi-factor authentication

Password management software allows users to store, organise and generate passwords for their user credentials (Brodkin, 2013). The use of a password management software tool is almost exclusively associated with respondents from the Information Technology sector Organisation: Password recollection (subsection 5.4.6). These results indicate that fourteen out of the sixteen respondents using a password management tool are involved in an Information Technology profession.

There is low usage of multi-factor authentication technology in the organisation according the results of the survey. The results showed only eighteen respondents (15.38%) are using multi-factor authentication (section 5.4.8). The majority of these respondents (77.78%) are once again from the Information Technology sector.

5.4.11 Review of analysis

The results from the survey indicated that most of the respondents are familiar with password policies in their professional or academic capacity. They are aware of the need to regularly change their passwords and select a minimum number of alphabetic and

numeric character based passwords. Furthermore, they are prevented from reusing the same password consecutively due to the enforcing of password history tracking.

The respondents mostly have five or fewer user accounts that they use within their organisation. Most of the respondents manage the passwords for these accounts by either memorising their passwords or by reusing the same password on all their accounts. The use of a password management tool is almost exclusively associated with respondents from the Information Technology sector.

The methods of managing and organising the respondents' credentials are mainly by memorising their credentials or reusing the same password on different accounts. This may be a result of the fact that most of the respondents have very few accounts to manage. There are, however, better methods for credential management: simply put, a password management tool. These password management tools are primarily employed by respondents from the Information Security sector. The same results applied for the use of multi-factor authentication technologies; the majority of the respondents using it were from the IT sector as well.

The reusing of passwords on different accounts is a common occurrence, as demonstrated by the results of the survey. Password reuse has become a common method for memorising credentials for user accounts at the expense of security (Duggan *et al.*, 2012). The potential dangers of reusing a common password will be discussed further in section 5.6.

Table 5.4: Summary of findings for organisation password management

Significant Findings	Result	Percentage
Password length	Between five and eight characters	76.74%
Password expiration	Every 30 Days	58.33%
Password complexity	alphabetic and numeric character	78.79%
Password history and tracking	Tracked and prevented from using prior password	51.52%
Number of user accounts	One to five accounts	82.05%
Password reuse	Reusing passwords on different accounts	67.52%
Method for remembering passwords	Password reuse	37.61%
Password shared with colleagues	Yes	32.48%
Knowledge of colleagues password	Yes	39.32%
Multi-factor authentication	Not being used	64.96%
Security awareness training	Training not provided by organisation	72.00%

Security awareness training is not being provided to the majority of the respondents. Awareness programmes are designed to educate computer and network users as to how

they can better protect themselves and their organisation from information security breaches. Table 5.4 summarises all the significant findings from the survey data on password management in the organisation.

The respondents were familiar with password practices enforced within their organisations. The next section (section 5.5) will explore password management habits when managing personal internet and computer accounts.

5.5 Personal password management and habits

The survey included a section of questions pertaining to the respondents' password management habits in a personal capacity. The questions were designed to ascertain the level of concern the respondents have towards the privacy and security of their user credentials. The survey questions (Questions 33 to 55), for this section are available in Appendix A.

5.5.1 Password length

The respondents were asked about the number of characters they used for their account passwords. Longer passwords with more characters have a higher entropy and more secure (Wiberg, 2011). The more characters a password has, the higher the strength and the longer it will take to crack the password (Florencio and Herley, 2007). The results showed that the bulk of the respondents fall into two equal groups of 45.3% each. These two groups used either five to eight characters or nine to fifteen characters respectively.

5.5.2 Password expiration

Organisations commonly enforce the changing of passwords on a regular basis. The respondents were questioned as to how often they change their private account passwords. 31.62% indicated that they never change the password associated with their personal accounts. The remaining results were as follows: 26.5% change their password every twelve months or longer; 19.66% every six to twelve months; and 14.53% change their passwords every three to six months. Only 7.69% change their private account password at least once a month. This is represented in the Figure 5.4.

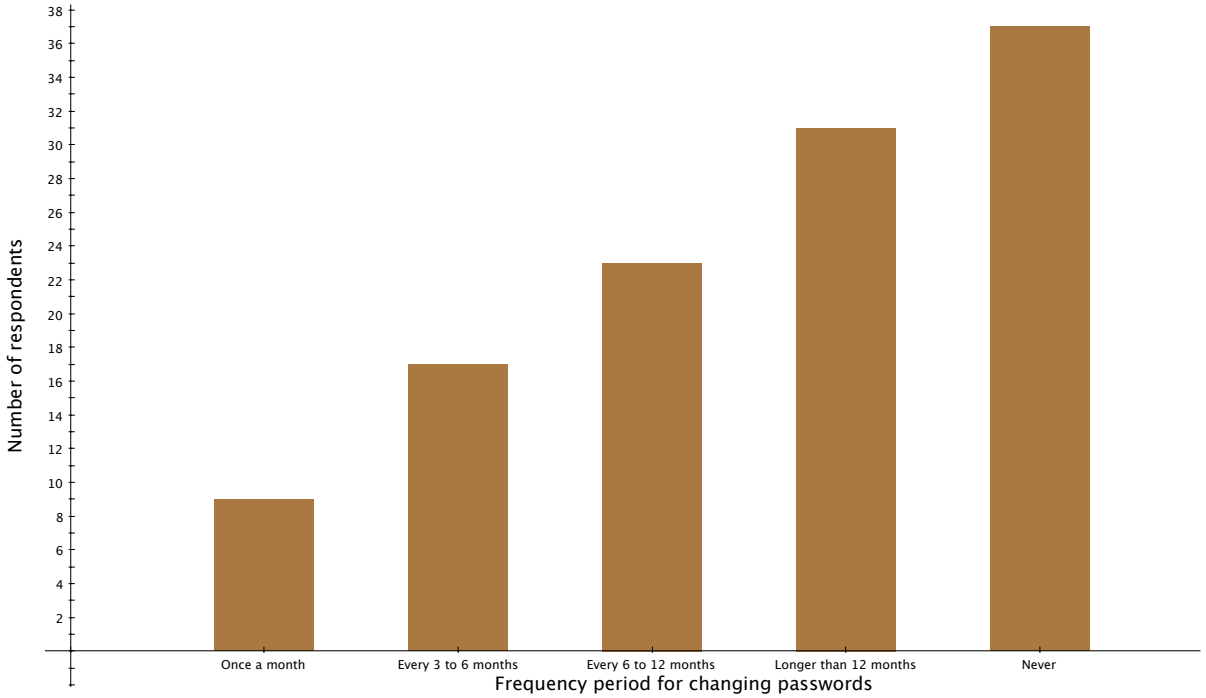

Figure 5.4: Frequency respondents change their personal passwords

5.5.3 Password complexity

The strength of the password is increased when it is more complex because it becomes less easy to crack or guess (Ur, Kelley, Komanduri, Lee, Maass, Mazurek, Passaro, Shay, Vidas, Bauer, Christin, and Cranor, 2012). The complexity will be affected both by the types of character used and the words or phrases included in the password.

Character types The respondents were presented with a question regarding the types of characters they use to compose their personal passwords. The results from the survey showed that 32.48% use alphabetic characters (in both upper and lower case) and numbers and special characters (e.g.,!@#$%^\&) to formulate their passwords. The next composition of characters are number and letters together; this was the choice of 29.06% of the respondents. The dataset also indicated 25.64% of respondents use alphabetic characters, numbers and special characters.

Dictionary words Concerning the use of dictionary words as or as part of their passwords, 25.64% responded that they did use them.

Personal information The respondents were asked whether or not they include personally identifiable information as part their password composition, with 46.01% answering affirmatively. The respondents who did indicate that they use personal information as part of their passwords were questioned about what information they chose to include. The 55 respondents were presented with a multiple selection of answers from which to choose. 55.17% indicated that they use names of people (family members, work colleagues and celebrities, for example) and 50% responded that they use special dates (birthdays or anniversaries). The results also indicated that 37.93% include numbers that are special to them; these could be lucky numbers, ATM pin numbers or even their identification number.

5.5.4 Number of user accounts and password reuse

The results from the questions relating to the number of user accounts managed by the respondents and whether or not they reuse the same passwords on different accounts are as follows:

Number of user accounts 50.43% of the respondents manage four to eight personal accounts. 25.64% have from nine to fifteen user accounts. And 12.82% manage twenty or more personal user accounts.

Password reuse The majority of the respondents indicated that they do reuse the same password on different accounts. This result constituted 79.49% of the respondents.

These respondents then indicated as to how often and how many accounts would have the same password associated with it. 28.42% indicated that they used the same password on all their accounts. Another 28.42% also admitted using the same password on most of their accounts, but used a different password on accounts they deemed more important. The dataset also showed that 24.21% will use the same password on three or fewer accounts and then select a new password for the next group of user accounts.

Unique passwords The survey results showed that respondents predominantly have between one and three unique passwords for their personal accounts. The dataset indicates that 49.57% use from one to three unique passwords, 35.04% use from four to eight unique passwords, and 8.55% use fifteen or more unique passwords. The use of unique passwords for each personal account will reduce the number of times a user reuses the same password.

5.5.5 Password recollection

Computer and internet users are required to remember a number of user credentials for their personal accounts. The respondents were asked how they manage the usernames and passwords for all of their accounts. The respondents that try to memorise all their passwords accounted for 36.75%, while 30.77% reuse the same password on most of their accounts in order to remember the password, and 15.38% use password management software.

Frequency for forgotten passwords The survey respondents were asked how often they forgot their passwords and how many passwords need to be reset every year. 49.57% indicated that they rarely forgot their passwords and required no more than one password to be reset per a year. It was also determined that 43.59% seldom forget their password and required two to five of their passwords reset per year.

Password recovery It is common practice for internet websites to provide a facility for their users to retrieve and/or reset their credential passwords. The survey results indicated that 88.03% of the respondents have used a password recovery facility. The respondents were presented with a number of recovery methods that they could use to retrieve their forgotten passwords. The most commonly used method amongst the respondents was an email containing a link to reset their user password: 66.67% indicated they had used this process. 57.14% of respondents revealed that they had been asked a number of security questions to retrieve their passwords.

5.5.6 Password disclosure

The respondents were asked whether or not they had ever shared any of their personal user credentials with anyone, either deliberately or by accident. 38.46% indicated that they had shared their credentials. These respondents were then asked an additional question as to whether or not they then changed the password after they had disclosed it or discovered they had disclosed it; 61.54% admitted that they did not change it.

5.5.7 Multi-factor authentication

There are a number of multi-factor authentication technologies that can be integrated into the authentication process of the website login (O'Gorman, 2003). The respondents were asked whether or not they ever experienced any of these technologies such as a tokens or one time passwords via SMS. Nearly half the respondents (48.72%) indicated that they had encountered multi-factor authentication technology combined with their user account logins.

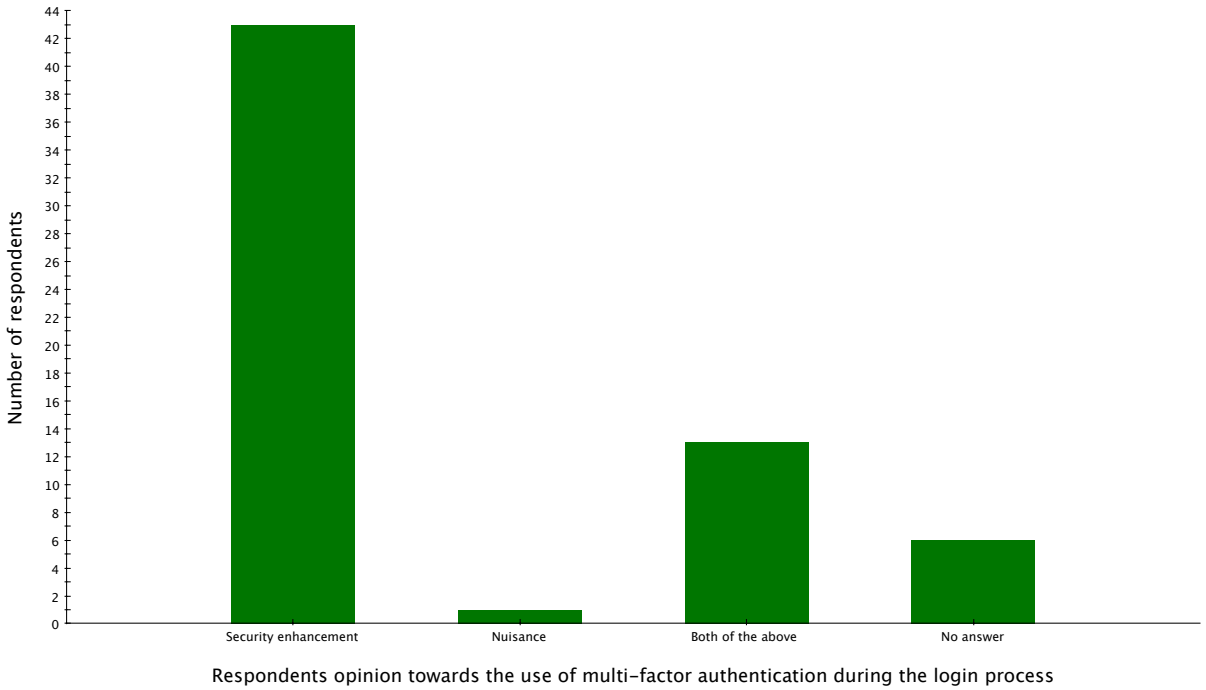

Figure 5.5: Respondents sentiment towards multi-factor authentication

The respondents who had used multi-factor technology were also asked what their attitude was towards the inclusion of this technology. 68.25% indicated that they believed it was a security enhancement, 20.63% indicated that it was both a security enhancement and a nuisance while logging on, and only 1 respondent indicated that it was purely a nuisance value during the authentication process. The graph Figure 5.5 displays the results of this enquiry.

5.5.8 Analysis

The dataset results show that the majority of the respondents (90.6%) use either five to eight or nine to fifteen characters when creating their passwords (section 5.5.1) for

their personal accounts. The length of the password effects the strength of the password (Komanduri *et al.*, 2011). Passwords less than eight characters are considered 'weak', while passwords of fifteen characters or more are considered between 'medium' strength up to 'strong' passwords (Scarfone and Souppaya, 2011).

The complexity of the password will also affect the strength of the password. The results indicated that the majority of respondents (58.12%) are using either a blend of characters (which includes alphanumeric, special characters and different letter cases) or they are using a combination of only letters and numbers (section 5.5.3). The complexity of the password is greatly increased when using more character types and changing the letter case of the alphabetic characters. Passwords that contain only letters and numbers are less secure (Klein, 1990).

The greater part of respondents revealed that they either never change their private passwords or they change them, at the earliest, every twelve months (section 5.5.2). The respondents may never, or infrequently, change the passwords of their personal account because they are not forced to or simply do not feel it is necessary to do so. The online services or website that they use may not have a policy to enforce this practice.

The minority of respondents indicated that they had previously, either deliberately or unintentionally, shared their password with someone else (section 5.5.6). The majority of this dataset did not change their password after the disclosure event. There is a clear indication that respondents do not favour changing their passwords, whether on a regular basis or even in the occasional event that someone knows their password.

The bulk of the respondents (76.07%) have anywhere from four to fifteen user accounts they use in a private capacity. The results from section 5.5.4 demonstrated that the preponderance of respondents reuse the same password on most of their accounts and that they have very few unique passwords that they use for their user credentials. The small number of unique passwords also supports the finding that the respondents will use the same password on many accounts but will use a different password on accounts they deem to be more important. The reuse of passwords on all user accounts often proves to be a perilous approach to password management (Ives *et al.*, 2004).

The results of the survey show that password recollection methods are dominated by two types: 1) memorising all of the passwords and 2) reusing the same password on most of the accounts. The analysis shows that nearly 40% of the respondents who memorise their passwords use only letters and numbers when creating their passwords. These character sets reduce the complexity and overall strength of the password.

Managing user names and passwords can be difficult with a large number of user credentials. A password management software tool is a good method for accomplishing this task. The analysis shows that 83.33% of the respondents who use a password management tool are from the Information Technology sector.

Multi-factor authentication requires a user to input an additional verification parameter when completing the authentication process. Nearly half of the respondents (48.72%) were familiar with this technology and the bulk of them (68.25%) indicated that they believe it was an enhancement to the security access control process. 35 of 57 respondents (61.4%) who are using multi-factor authentication are also from the Information Technology sector.

5.5.9 Review of analysis

The survey data sets have revealed a good deal of information about the habits of the respondents when it comes to password management of their private user accounts. The respondents almost never or very frequently change their passwords, even when they are aware that it has been disclosed to another person. The summary of the survey findings for personal password management is shown in Table 5.5

The results show that there are varying degrees of complexity being used by respondents on their passwords. The respondents do, however, tend to frequently reuse the same password on many of their accounts. The more complex the password is, the stronger it is, and thus more difficult to guess (Burnett and Kleiman, 2006). The problem of reusing the same password, however, can greatly increase the risk of the user accounts being comprised. Even if the user does use a strong, complex password, the theft or disclosure of that one password could compromise *all* of their accounts.

The respondents also indicated that their primary methods for recalling their passwords are either to memorise all their passwords or reuse the same password. The analysis of the respondents that did try to memorise all their passwords showed they used a reduced set of character types mainly composed of letters and numbers only.

As in the section 5.4.10 the majority of participants using multi-factor authentication and password management software are from the Information Technology sector. These respondents are using additional tools and technology to increase their private user account security.

Table 5.5: Summary of findings for personal password management

Significant Findings	Result	Percentage
Password length	(five and eight) or (nine to fifteen) characters	90.60%
Password expiration	Never change passwords	31.62%
Password complexity	Alphabetic characters (in upper and lower case), numbers and special character	32.48%
Number of user accounts	Four to eight accounts	50.43%
Password reuse	Reusing passwords on different accounts	79.49%
Method for remembering passwords	Memorise all their passwords	36.75%
Password shared with others	Yes	38.46%
Changed password after sharing it	No	61.54%
Multi-factor authentication	Not being used	51.28%

5.6 Password reuse analysis

There is real danger when internet users use the same password (and sometimes the same username) on different internet services. Criminals that have acquired a person's user credentials can use the stolen username and password to gain unauthorised access to other websites where the same password has been reused.

Previous research has shown that internet users are using the same passwords on different internet accounts. This was the case when security researcher Troy Hunt compared the list of stolen user credentials between Sony and Yahoo Voices (Hunt, 2012). The researcher showed that 59% of users that had accounts at both Sony and Yahoo were using the same password on both services. There are a number of survey results that show password reuse is commonplace amongst internet users. The Microsoft study on users' password habits (Florencio and Herley, 2007) showed that users are reusing the more passwords more often as their number of user accounts increase.

There are reports that stolen user credentials are being used to compromise other accounts. This was the case with Best Buy customers who had their online accounts accessed by hackers: gifts were then being purchased for unauthorised recipients (Fontana, 2012). Best Buy revealed that these compromised account were being accessed with the use of stolen credentials from other breached internet websites from users that had the same passwords on both websites. The password reuse habit of internet users can create a 'Domino Effect' of insecurity (Ives *et al.*, 2004). The attack on Mat Honan's online accounts (Honan, 2012) clearly demonstrated that linking account details can allow

hackers to systematically gain access to each of the victim's accounts and completely devastate all of that individual's information. If the password for all these accounts is the same, this process is profusely easy to accomplish.

Previous studies such as Tamil *et al.* (2007) and (Notoatmodjo and Thomborson, 2009) have demonstrated that password reuse is a common management technique for internet users. Cyber criminals have managed to steal massive password databases, as in the case of Linkedin (Kamp, 2012) and Adobe (Kale, 2013), and now have the ability to cross reference millions of user details and determine whether or not users have used the same credentials on multiple stolen accounts. The survey questions (Questions 23, 24, 34, 37 and 38), for this section are available in Appendix A.

5.6.1 Analysis

From the outset of the research, one of the objectives was to determine whether or not password policies within an organisation or institution had any effect on the participants (section 1.4). This research demonstrates that the participants are not prevented from reusing nor informed not to reuse their passwords within their organisations. Password reuse is also a common habit displayed by the participants in personal password management. These findings are similar to previous studies such as (Florencio and Herley, 2007) and (Riley, 2006).

The respondents were asked whether or not they reuse the same password on multiple accounts. The question was asked both in the professional or academic context as well as in the personal context: respondents that did reuse passwords were 67.52% and 79.49% respectively. This showed a notable increase in password reuse between the two contexts.

The method of remembering passwords was addressed during the survey with questions asking the respondents how they remember their passwords for their user credentials. The results showed that 37.61% reuse the same passwords within their organisation and 30.77% reuse the same password in a personal capacity. These results confirmed that password reuse is a significant method applied by the respondents to remember their passwords.

Password reuse comparison with number of user accounts

The comparison of the number of personal accounts compared to the number of respondents who reuse passwords is shown in Table 5.6. The results indicate that password

reuse is lower with respondents managing fewer accounts such as respondents with only one to three accounts. The reuse usage increased as the number of accounts needing to be managed increased. The trend for this result continued up until respondents indicating they managed between sixteen to twenty accounts. The reuse percentage decreased at this point in the results and continued to do so for respondents with twenty or more accounts. The dataset indicates that the majority of users were managing from four to twenty user accounts and over 80% were reusing the same passwords.

Table 5.6: Number of account with password reuse percentages N=117

Number of user accounts	Percentage that are reusing passwords	Percentage of Total Respondents
1 to 3 accounts	40%	4.27%
4 to 8 accounts	86.44%	50.43%
9 to 20 accounts	86.67%	25.64%
16 to 20 accounts	75%	6.84%
20 or more accounts	53.33%	12.82%

The rate of password reuse increases as the number user accounts increase. This finding is similar to previous studies such as (Gaw and Felten, 2006) and (Florencio and Herley, 2007). These studies showed that their participants employed this tactic as it was the easiest method for remembering passwords for numerous user accounts.

Password reuse comparison with password management software

The results in Table 5.7 indicate that more of the respondents are using password management software as their number of user accounts increased. These results are particularly notable for the datasets of four to eight, nine to twenty and twenty or more accounts. There was also a significant decrease in the password reuse usage for respondents with more than twenty user accounts. This dataset also had the highest password management software usage with 40% of the respondents indicating that they did indeed use such software.

The results indicate that 15.38% of the overall respondents use password management software. The majority of these respondents are either studying or working in the Information Security sector (83.33%). The results for this dataset indicate similar password reuse rates within the organisation and in a personal capacity, 33.33% and 38.89% respectively. These results indicate a lesser password reuse percentage than the median of the overall results.

Table 5.7: Account with password management software usage N=18

Number of user accounts	Password management software is being used	Percentage of Total Respondents
1 to 3 accounts	20%	4.27%
4 to 8 accounts	8.47%	50.43%
9 to 20 accounts	16.67%	25.64%
16 to 20 accounts	12.5%	6.84%
20 or more accounts	40%	12.82

5.6.2 Review of analysis

The insecure practice of reusing passwords on multiple user accounts is prominent amongst the respondents of the survey. The majority of respondents use this practice both in their professional/academic password management as well as in their personal capacity.

One of the primary reasons for reusing passwords points to the respondents' need to remember their passwords for all their user accounts. The number of user accounts is associated with the amount of password reuse taking place by the respondents. There is a high percentage of reuse with the largest dataset of user accounts, ranging from four to fifteen user accounts.

There is, however, a decrease in password reuse for respondents who revealed that they manage twenty or more user accounts. This dataset also has the highest usage of password management software. Password management software allows the user to securely store user credentials and generate unique and random passwords for each account (Brodkin, 2013). This method of storing and managing user credentials shows a reduction in the rate of password reuse.

The use of password management software is also predominately performed by respondents from the Information Security sector. This result was also highlighted in this section (section 5.4.11).

5.7 Password length analysis

It is a common practice amongst organisations and institutions to implement a minimum password length for their computer systems, applications and websites. This practice of enforcing that users create passwords with a minimum number of characters decreases

the ability to crack it and increases the security, even if there are no other password restrictions enforced by the computer system (Proctor, Lien, Vu, Schultz, and Salvendy, 2002). The increased number of characters in passwords increases the difficulty of cracking them and therefore increases the strength of such passwords (Ur *et al.*, 2012). The survey questions (Questions 15, 16 and 39), for this section are available in Appendix A.

5.7.1 Analysis

A comparative analysis of password length between professional and personal password management demonstrated that corporate password policies have more of a negative effect on the participant password length. Again, one of the research objectives was to determine whether or not corporate password policies affect personal password management (section 1.4).

The majority of the participants (84.85%) indicated that their past or current organisation or institution enforces a minimum number of password characters as part of its security policy.

The bulk of the participants (76.74%) suggested that their password policy required them to use between five and eight characters when selecting their passwords. The dataset also revealed that 15.48% are forced to use between nine and fifteen characters in their passwords. Only 2.33% indicated that they are restricted to use between one and four characters, and none of the participants indicated that they are required to use fifteen or more characters.

The analysis of the participants' responses regarding the number of characters they use in their personal accounts differed significantly from their organisation password requirements.

The participants' results indicated that 45.3% use between five and eight characters in their personal capacity. And 45.3% also use between nine and fifteen characters in their personal capacity. A mere 9.4% use fifteen or more characters.

Nearly 36.36% of the participants indicated they are required to use between five and eight characters within their organisation, but then selected between nine and fifteen characters for their personal account passwords. Table 5.8 presents a comparison between the number of characters selected for organisational usage compared to the number of characters used in personal capacity.

Table 5.8: Password length between professional/academic and personal usage N=84

Number of characters used	Organisation/Institution Usage	Personal Usage
1 to 4	2.33%	0.0%
5 to 8	76.74%	45.3%%
9 to 15	18.61%	45.3%
15 or more	0.0%	9.4%
No Answer	2.33%	0.0%

The respondents who indicated that they use between sixteen and twenty characters as well as fifteen or more characters were compromised of participants using password management software and were from the Information Technology industry.

A substantial 70.94% of the participants also indicated that they believed that the number of characters in a password contribute to the increasing the strength of the password.

5.7.2 Review of analysis

The preponderance of the participants (84.85%) have been subject to a security policy within an organisation that requires them to have a minimum password length. The participants also have the knowledge and understanding that a longer password increases the security and strength of a password.

The majority of participants also indicated that they are required to have a password between five and eight characters long for their organisations' password access control. However, the average password length in their personal capacity was higher as more participants indicated they use between nine and fifteen characters.

These results indicate the organisations' password policies are encouraging participants to use even shorter passwords than they choose to use for their private online services such as email, social networks or e-commerce websites. This result could also reveal that corporates and institutions are not imposing password length requirements which are as secure as internet companies and online services.

5.8 Password complexity analysis

Users will create passwords that are easier for them to recall but consequently are easy guess. This occurrence has been proven in past studies of user password behaviour and

creation (Proctor *et al.*, 2002), (Bishop and Klein, 1995).

These studies have shown that even with password restrictions in place, such as password length or character types, users still create common words or phrases which are simpler to crack through the use of a password checking algorithm. The selection of more complexly formulated passwords increases the strength of such passwords.

The studies of password creation also showed that longer and more complex passwords were more difficult for the participants to recall (Proctor *et al.*, 2002). The survey questions (Questions 19, 21, 42, 43, 44 and 47), for this section are available in Appendix A.

5.8.1 Analysis

The results from the analysis of the survey data revealed that 78.79% of the participants who are subject to a password restriction policy in their organisation have to use alphanumeric passwords, and 67.68% also indicated that they were restricted from using names or dictionary words in their organisation.

In the context of their personal passwords, nearly half of the participants (47.01%) indicated they use personally identifiable information as part of their password formulation. The most commonly selected personal information attributes were names of people, special dates (birthdays, anniversaries), and special numbers (lucky numbers, ID numbers).

Only nine of the participants (7.69%) indicated the use their ATM pin number as a password for their user accounts.

The participants were asked to select the character types that they used to formulate their passwords. The most commonly selected character types, in descending order, were *Letters (Upper and lower-case) Numbers and Special Characters*, *Letters and Numbers*and *Letters, Numbers and Special Characters.* A list of the character groups and samples can be reviewed in Appendix B.

These results are shown in Figure 5.6. The most commonly selected character type set, namely *Letters (Upper and lower-case) Numbers and Special Characters*, is mostly composed of participants from the Information Technology industry (65.79%).

The analysis of the dataset shows that of participants who indicated they use personal information as part of their password, 32.67% are in the Information Technology industry.

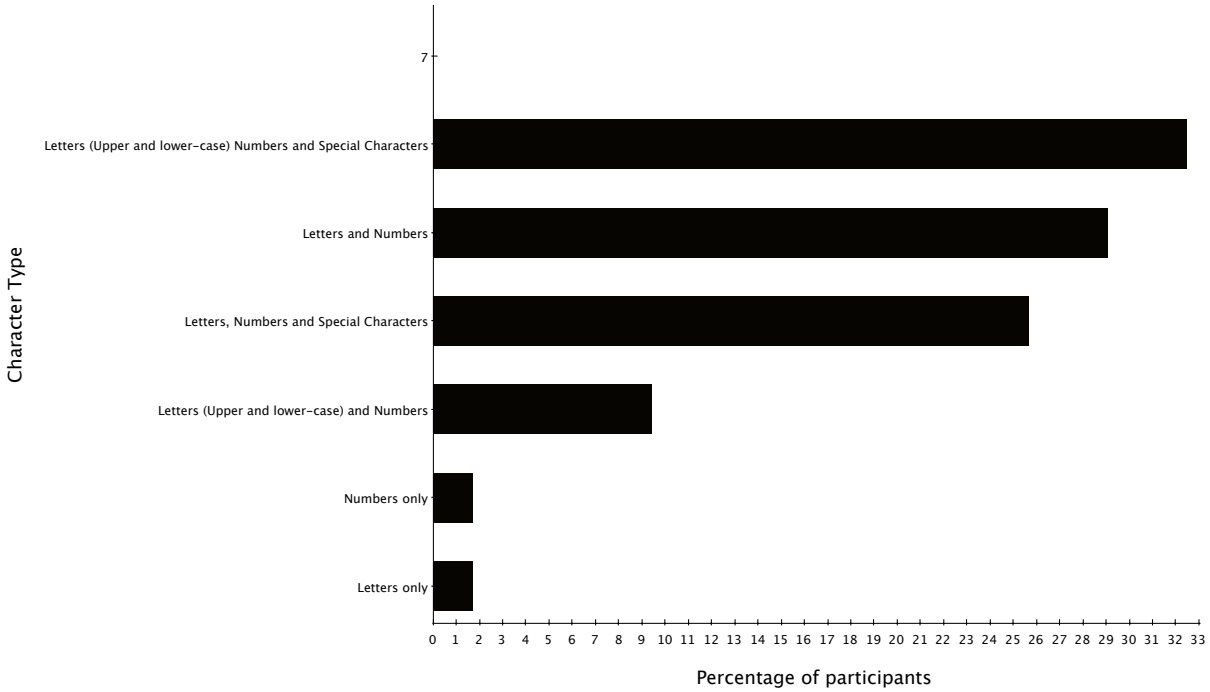

Figure 5.6: Character type selection by participants

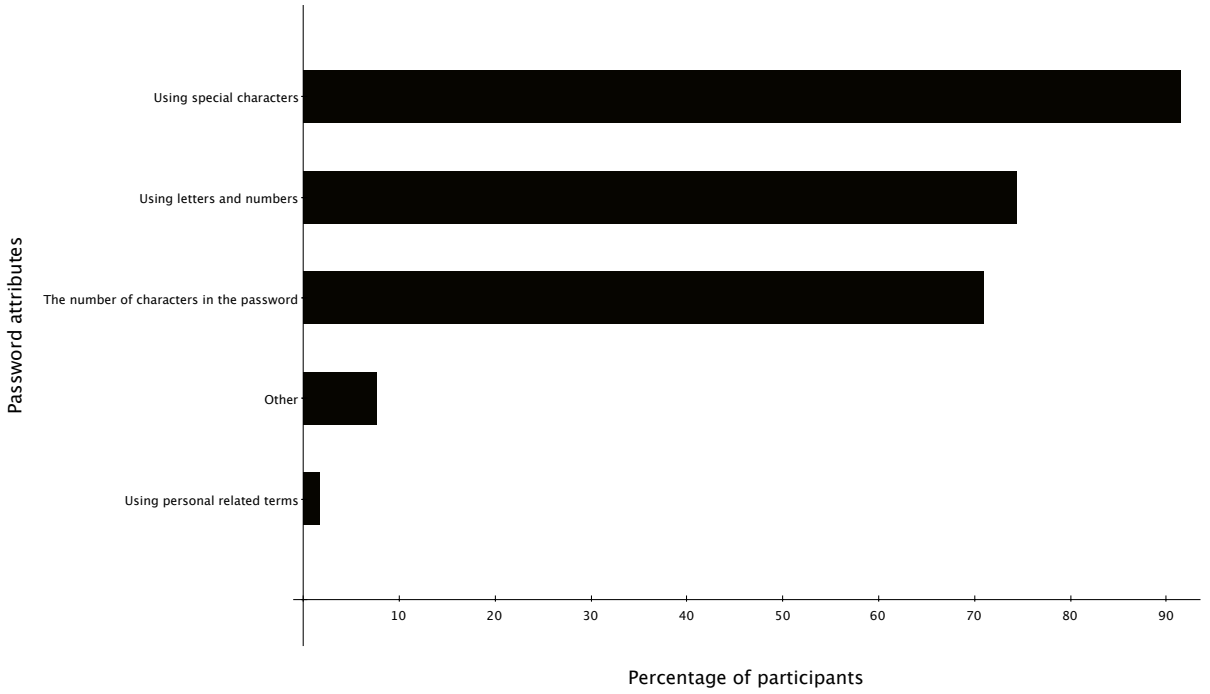

Figure 5.7: Password attributes that strengthen passwords

The most commonly used character type set are *Letters and Numbers* (38.18%). *Letters (Upper and lower-case) Numbers and Special Characters* and *Letters, Numbers and Special Characters* were used by 25.45% each.

This same datset also indicated that 50.1% use between five and eight characters, while 43.64% use between nine and fifteen character for their passwords. Section indicates that participants rarely or seldom forgot their passwords.

The Figure 5.7 displays the results indicating which attributes of a password increase the strength of it. Participants were able to select multiple options from the survey questions. The bulk of the participants indicated that using special characters, letter and numbers, and the number of characters increases the strength of the password. Only 1.71% believed that using personal information increased the password strength.

5.8.2 Review of analysis

The analysis of the complexity has shown that participants have been exposed to password restriction on their password composition. The use of alphanumeric passwords is a common requirement and dictionary words are commonly prohibited.

The use of personal information in passwords was considered not to be an attribute of strength by 98% of the participants, yet nearly 50% indicated they use it anyway in their passwords.

Nearly half of the participants use personal information as a part of their password construction. These participants were mostly from a non-Information Technology background, most commonly using only letters and numbers for their passwords and averaging between five and fifteen characters in their passwords.

These participants rarely or seldom forget their passwords. Previous studies have shown that as passwords get longer and more complex, the user's ability to recall these passwords reduces (Pilar *et al.*, 2012), (Bishop and Klein, 1995).

5.9 Password management tools/services analysis

Internet and computer users have the challenging task of having to manage a number of user account credentials and passwords. The industry of software developers have

designed and developed a number secure password management software tools. These password managers are essentially a database of usernames and passwords.

These password management tools provide the user with the ability to store and retrieve their credentials for any of their user accounts. These tools also provide features such as randomly generated passwords and automatic form-filling for online form pages. The adoption of a password manager has been endorsed by renown security professionals such as Bruce Schneier (Schneier, 2010) and Steve Gibson (Gibson and Laporte, 2010).

Studies have shown that problems with password management tools presents more of a usability and practicality issue (Chiasson *et al.*, 2006) (Karole *et al.*, 2011). Users may find these tools to be cumbersome and complicated. The users may also not trust the tool and believe that storing the password in their memory is more viable and secure solution. The survey questions (Questions 24,34 and 35), for this section are available in Appendix A.

5.9.1 Analysis

An analysis of the survey dataset was conducted to compare the password usage and generation behaviour of the participants who both used and did not use password management software. The analysis was conducted on the participants' personal password usage and habits. The participants could be in one of two groups: Group A use password managers, while Group B do not.

Only 18 out of the 117 participants (15.38%) indicated that they used a password manager (Group A). These participants were almost exclusively from the Information Technology sector (83.33%). The majority of Group A (77.78%) indicated that their security and privacy were of great concern and employed the highest level of protection. The majority of Group B (51.04%) tended to be less concerned, but still endeavoured to protect their passwords to the best of their ability.

The results indicated that participants of Group A predominantly had more accounts to manage than participants in Group B. A notable 66.67% of Group A participants had between nine and twenty (or more) user accounts, while 84.38% of participants from Group B had between one and fifteen user accounts to maintain.

The survey results showed that Group A participants reused passwords less than Group B participants. These results indicated that 38.89% of Group A users reused passwords.

The percentage was much higher with participants of Group B, with 87.5% indicating that they did indeed reuse passwords.

Group A results also showed that the participants have more unique passwords than Group B participants. This is related to the fact that Group A participants did not reuse passwords as often as Group B and would regularly use a different password for each of their accounts. 38.89% of Group A participants had fifteen or more unique passwords and 33.33% had four to eight unique passwords. Group B only had 2.08% of its participants using fifteen or more unique passwords while the majority (57.29%) had only one to three unique passwords.

Group A had nearly 40% of the participants using twenty or more characters in their passwords, while Group B participants had a mere 1% using twenty or more characters in their passwords. Group A had 44.45% of the participants using between nine and twenty characters while Group B had 96.87% using between five and fifteen characters.

The analysis of password composition indicates that the majority (77.78%) of Group A are using letters in both upper and lower case, and numbers and special characters to formulate their passwords. Group B participants are predominantly using only letters and numbers (35.42%).

5.9.2 Review of analysis

Very few of the participants have adopted the practice of using a password management tool for storing, retrieving and generating their passwords. The majority of the users who do employ this practice are Information Technology professionals who are likely to have had more exposure to these technologies.

The overall comparison indicated that users of password managers tend have more accounts than users without passwords managers. Their password reuse is lower and as a result of this have more unique passwords as well. A summary of results for the participants not using password management software are displayed in Table 5.9 and a summary of participants that are using password managers are displayed in Table 5.10.

It was determined that participants with password managers have longer passwords with more characters. They also have passwords formulated with more complexity as they mix a variety of character types including upper and lower case and special characters (see Appendix B). Participants without password managers most commonly use only letters

and numbers. Using longer and more complex passwords improved the security of the user accounts. In Appendix B the list displays a benchmark for password cracking based on the possible combinations of the number of character and types of characters in a password.

Table 5.9: Password behaviour for participants not using password managers N=99

Password attribute	Most frequently selected attribute	Percentage
Number of accounts	4 to 8	56.25%
Regularly reuse passwords	Yes	87.50%
Number of unique passwords	1 to 3	57.29%
Number of characters	5 to 8	51.04%
Password composition	Letters and Number only	35.42%

Table 5.10: Password behaviour for participants using password managers N=18

Password attribute	Most frequently selected attribute	Percentage
Number of accounts	20 or more	33.33%
Regularly reuse passwords	No	38.89%
Number of unique passwords	15 or more	38.89%
Number of characters	(9 to 15) and (20 or more)	38.89%
Password composition	Letters (Upper and lower-case) Numbers and Special Characters	77.78%

5.10 Multi-factor authentication analysis

Multi-factor authentication provides an enhancement to the user authentication process as the authentication process will require the user to provide an additional component when logging in and authenticating on a computer system.

These additional components can be either "something the user knows" such as a one-time password system (OTP) (Haller, Metz, Nesser, and Straw, 1996). Secondly, another component of multi-factor authentication could be "something the user has" such as a token or smart card (Aussel, 2007). Finally, the authentication could also be "something that the user is" such as a biometric scanner for fingerprints or a retina (Boatwright and Luo, 2007).

The Information Technology industry has long maintained that usernames and passwords are not enough security for user authentication and so the adoption of these technologies

has increased in the past few years. Major internet websites such as Google,[1] Facebook[2] and Twitter[3] all offer a multi-factor authentication option to the users for logging on to their sites. The survey questions (Questions 27, 28, 48, 49, 60 and 61), for this section are available in Appendix A.

5.10.1 Analysis

The participants were presented with questions relating to the use of multi-factor authentication both in their organisation and personal capacity. The participants were questioned as to whether or not their organisation had implemented multi-factor technology. A mere 15.38% indicated that their organisation did use multi-factor authentication as a component of their authentication process. The participants also indicated that nearly half of them (48.72%) chose to use a form of multi-factor authentication in their personal computer security usage.

However, 19.66% of the participant selected "No answer" in response to the question relating to multi-factor usage in the organisation. This may imply either that the participants did not know what this technology is or perhaps that they were not aware they were indeed using it.

When asked what their perception of multi-factor authentication was, the participants could indicate whether it was a security enhancement, a nuisance or both of these. In both the professional and personal responses the clear majority of responses revealed that multi-factor authentication is considered a security enhancement. The results were 77.78% and 75.44% respectively.

The survey included questions relating to internet bank usage and the banks that the participants use for this service. Nearly 95% of the participants indicated that they did indeed use internet banking. All of the major five South African banks were selected by at least one of the participants and all of these employ a form of multi-factor authentication as part of the internet banking authentication process. ABSA[4], First National Bank[5],

[1] http://www.google.com/landing/2step
[2] https://www.facebook.com/note.php?note_id=10150172618258920
[3] https://blog.twitter.com/2013/getting-started-with-login-verification
[4] http://www.absa.co.za/Absacoza/Security-Centre/Online-Security/Absa-Online-Security-Measures
[5] https://www.online.fnb.co.za/rhelp0/zob/security/one_time_pin.htm

Nedbank[6], and Standard Bank[7] all used one-time password, while Capitec Bank[8] provides its customers with downloadable token software for their cellphones. These additional authentication requirements are mandatory for all of these banks' online banking services.

Just over half (52.14%) of the participants indicated that they believe, in general, that usernames and passwords are not sufficient enough protection for their online accounts. These participants were then asked to select the technologies that they believed would improve their security: 80.36% selected smart cards and tokens; 66.07% selected one-time passwords; 50% selected biometric scanners; and 46.43% selected certificate-based authentication.

5.10.2 Review of analysis

The results from the analysis into the usage of multi-factor authentication by the participants indicated that more of them are using this technology in a personal capacity than in the work or academic environment. The participants mostly perceived that this technology is a security enhancement to their authentication process and that it is less of a nuisance when logging onto their computer applications and websites.

All of the main banks in South Africa employ a form of multi-factor authentication with their online banking services. A comparative analysis of internet banking usage and multi-factor usage indicated that while almost all of the participants use internet banking services, only half of them indicated that they use multi-factor authentication in a personal capacity. The question on the survey specifically mentioned the use of a one-time password for internet banking - Appendix A (Question 48 and 49) .

The respondents who indicated that usernames and passwords are not adequate security, predominantly chose smart cards and/or tokens as the preferred technology to enhance their security authentication. The results displayed in Table 5.11 are of the preferred multi-factor authentication technologies. The participants were able to select multiple technologies from a pre-set list as well provide any additional technologies no on the list.

Participants' lack of awareness of these security technologies may be an indication of their lack of security awareness training and knowledge. The section on security awareness and training (section 5.11) may provide further insight into this.

[6]https://www.nedbank.co.za/website/content/promotions/index_detail.asp?PromoID=529

[7]http://www.standardbank.co.za/portal/site/standardbank/menuitem.de435aa54d374eb6fcb695665c9006a0/?vgnextoid=0544f8bc8f35b210VgnVCM100000c509600aRCRD

[8]http://www.capitecbank.co.za/personal-banking/internet-banking

Table 5.11: Preferred multi-factor technology selection by participants N=61

Multi-factor Authentication Technology	Percentage by participants
Smart cards and tokens	80.36%
One-time passwords	66.07%%
Biometrics	50%
Certificate based authentication	46.43%
Other	1%

5.11 Security awareness and training analysis

In an article titled "The Ten Commandments of Information Security Awareness Training" (Desman, 2003) the author writes that "Information security is a people, rather than a technical, issue."

Information security professionals use a number of technical tools such as firewalls and access control systems to protect an organisation's resources. The organisation must also train their employees how to participate in these security practices and provide ongoing education about potential security threats.

Employees should understand that their cooperation in adhering to these security practices will aid the organisation in preventing security breaches. Furthermore, employees should understand that the security policies are not implemented to hinder their workflow but rather to guide them to employ security best practices in general. The survey questions (Questions 29,57,58 and 59), for this section are available in Appendix A.

5.11.1 Analysis

One of the stated research objectives was to determine whether or not participant are receiving adequate security awareness training or any type of security awareness training at all (section 1.4). The findings demonstrate that very little training has been provided to the participants. The participants do, however, exhibit the understanding of secure password selection but fail to employ it as part of their password management practices. Further training would increase the participants' awareness of the threats associate with insecure passwords and may consequently increase the adoption of more secure password management.

The survey presented the participants with a question relating to formal security awareness training in their organisation or institution. Only 24.79% of the participants indicated

that their organisation provides security awareness training. These participants were then provided with a list of methods that were likely used by their organisation to promote security awareness. The participants were able to select multiple options from the list. The results indicated that 62.07% received security training upon joining the organisation. 44.83% received training through periodic refresher courses, email campaigns, posters and access to internet websites and blogs.

In relation to password specific security awareness, the participants were presented with a list of passwords of varying lengths and complexities. The strongest password contained alpha-numeric characters, special characters and upper and lower case characters. Elements that increased the strength of the password were removed from other example passwords, and the weakest password contained only lower-case letters (see Appendix B).

The list of passwords in order from strongest to weakest were as follows:

1. $#pL@n3tEARt4
2. H0t3L9098
3. Mustang10
4. antelope2
5. Apple

The participants had to rank the passwords in order from what they determined to be the strongest password to the weakest password. The participant count (and percentages) in Table 5.12 show the number of participants that ranked the listed password in the correct order of strength. The results in Table 5.12 indicated that the majority of the participants ranked each password in the correct order of strength (from strongest to weakest).

Table 5.12: Result of password strength ranking selected by participants N=117

Listed password	Count of participant	Percentage
$#pL@n3tEARt4	112	95.73%
H0t3L9098	109	93.16%
Mustang10	97	82.91%
antelope2	99	84.62%
apple	113	96.58%

The participants were then asked to list the same set of passwords according to their own likelihood of personal use. The participants had to rank the passwords in order from 'mostly likely to use' to 'least likely to use'. The results in Table 5.13 indicated that while the order of password strength remained the same, the usage percentage of the each password was lower than the determined strength.

The Table 5.13 displays the ranking order of the results from the mostly to least likely used password, with the highest count and percentage of participants for each selected password.

Table 5.13: Result of password usage ranking selected by participants N=117

Listed password	Count of participant	Percentage
$#pL@n3tEARt4	53	45.30%
H0t3L9098	51	43.59%
Mustang10	57	48.72%
antelope2	57	48.72%
apple	90	76.92%

5.11.2 Review of analysis

The analysis of the survey results revealed that the bulk of the participants had not received security awareness training at their organisation or institution.

The participants who had received training indicated that the majority of them had received an introductory security lesson upon joining their organisation. Fewer of the participants indicated that they had received ongoing training or refresher courses, or had been exposed to security awareness posters, email alerts or website information.

A comparative observation between the tables: Table 5.11 and Table 5.12 indicated a significant difference between the participants' knowledge about determining the strength of a password and how they actually choose to use that knowledge when creating their own passwords.

The bulk of the participants were able to determine the strength of the passwords and place them in the correct order from strongest to weakest. A substantial 93.16% of the participants were able to accomplish this exercise successfully.

There was a significant drop in the average to 48.72% when determining whether or not the participants would apply this knowledge to their own password selection and usage.

The results show there is a clear disconnect between the participants' knowledge of good password practices and their application of that knowledge.

5.12 Summary

The analysis of the survey results revealed similar findings to the related research in Chapter 3. The participants of this survey employed insecure password management habits such as short and simple passwords. The participants also regularly reused the same password on many of their user accounts, significantly increasing vulnerability to the threats associated with password reuse.

The participants lacked security awareness knowledge and seldom received training on this from their organisations or institutions. The use of password management software is not common amongst the participants despite the fact that results have clearly shown that using this software leads to more secure password management practices.

The implementation of password policies within their organisations has not improved the password management habits of the participants and in some cases (such as with password length and multi-factor authentication usage), personal password practices are more secure than professional ones.

The use of multi-factor authentication is considered a security enhancement by many of the participants; however, adoption and use of these technologies is quite low. The participants exhibit a good knowledge and understanding of the strength of passwords but many fail to employ this knowledge when choosing their passwords.

Further discussions concerning the findings of this research are detailed in the final chapter. The researcher reviews the findings of this study and presents conclusion based on those findings.

Chapter 6

Conclusion

6.1 Summary of Findings

The survey analysis reveals that participants are composed of students and employed professionals. The students are mostly between the ages of 19 to 25 while the employed participants are predominantly between the ages of 26 to 45.

The participants are responsible for managing a number of user account credentials both in their professional or academic context as well as in their personal capacity. The participants have displayed a fundamental understanding they need to be security conscious about their usernames and passwords; however, their opinions are divided about usernames and passwords being adequate enough security to protect access to their computer systems.

The bulk of the participants are familiar with password restriction policies that have been implemented in their organisation or institutions, password policies which include restriction on the number of characters, the types of characters, expiration of passwords, and the tracking of previously used passwords. The participants' most common methods for password recollection are memorising their passwords or simply reusing the same password on multiple accounts.

The implementation and use of multi-factor authentication technologies within organisations and institutions is not common. The results also showed that security awareness training is not being provided on a regular basis either.

The analysis of participant password usage habits in their personal capacity revealed that the majority are reusing passwords across multiple accounts. This finding is also further substantiated as the participants most commonly use their memory to store and recall their passwords. Further to this, the majority of participants indicated that they seldomly forget their passwords.

The practice of reusing passwords across multiple accounts is high both in organisations and in personal account management. Participants are prone to this habit as it connects to their reliance on memory for remembering their passwords. Participants using password manager software are less prone to the reuse habit and are primarily Information Technology professionals or students.

A minimum password length is a common restriction implemented by organisations and institutions. An observation of the average number of characters in passwords used in the professional and academic context as compared to the personal context shows that participants use longer passwords in their personal passwords.

The complexity requirements of the participants' passwords are enforced in their organisations and institutions. Participants do have an understanding that creating passwords containing a variety of different character types is more secure. Even so, participants regularly include personally identifiable information in their passwords.

The use of a password management software tool is not a common practice amongst the participants. These tools aid users in storing and recalling their passwords. Participants that use password managers generally practice better password management methods than participants who don't. These preferred practices include using stronger passwords, managing more user accounts and less reusing of passwords.

Multi-factor authentication is more commonly used in the personal capacity than within organisations or institutions. Almost the entire participant sample indicated that they use online internet banking services where multi-factor authentication is required, but nearly half still did not indicate they are using this technology.

The results of the security awareness analysis showed that the bulk of the participants do not receive training in their organisation or institution. While participants were able to demonstrate an ability to judge password strength, most did not actually apply this knowledge when creating their own passwords.

6.2 Conclusions

The researcher set out to determine whether or not users from corporate and academic backgrounds are security aware when it comes to creating, storing and recalling their passwords. The study was exploratory in nature and intended to be used in comparison to similar studies conducted around the world.

The results from this research show a similar pattern of poor password management to those demonstrated in the literature review from previous password surveys Chapter 3. This study was conducted with South African participants only and the results are comparable to other surveys conducted globally.

The participants of this survey demonstrated the necessary knowledge and understanding of poor password management; however, as found in other studies, the majority neglected to apply this knowledge to their own password management methodology. In fact, most of the participants are simply not practicing good password management.

Participants' are knowledgeable of the security threats surrounding poor password management and yet a lack of implementation can be attributed primarily due to one reason: the participants have simply been told to adhere to a set of rules without really understanding *why* it is imperative to do so.

The participants frequently reuse the same password on multiple accounts. This is a common method of password recollection for many of the participants who need to manage a large number of user accounts. This, in conjunction with password policies to which the participants are subject, inevitably forces the users to create a small group of passwords that get reused a number of times. The dangers of this practice can create a 'domino effect' whereby one stolen set of credentials is likely to lead to a complete breach of all the user's internet and computer accounts.

The participants have worked or studied in a computer environment where system policies and processes require users to adhere to restriction concerning password usage. It has been seen a previous study (Inglesant and Sasse, 2010) that password policies within the organisation can be frustrating for users and can in fact be counterintuitive for the users. The participants of this study have shown that these organisational password policies do not improve their password management practices and in some aspects are actually worse than their personal password practices.

The results from the analysis of password length (section 5.7), revealed that participants' average password lengths were longer in their personal passwords than in their professional and academic passwords. This finding was attributed to the fact that many of the participants' organisations and institutions enforce a lower character length requirement than their personal internet accounts.

The majority of the participants are not being provided with technologies for improving their access control security in their organisation or institutions. Technologies such as smart cards, one-time passwords or tokens are not commonly available to the participants and the participants are aware that they do provide a security enhancement. In their personal capacity, however, these technologies are more abundantly provided and used by the participants. All of the major banks in South Africa provide this additional access control process (section 5.10). Again, though, many of the participants did not even realise they were using such technologies

In addition to the lack of security enhancement technologies, organisations and institutions are not providing enough security awareness training, nor are they providing such training on an ongoing basis. This lack of training is certainly not benefitting the participants. The participants clearly demonstrated this fact by being able to identify password strengths but failing to use this strength tactic themselves (section 5.11).

An element that has been shown to improve password management habits of participants is the use of a password manager tool (section 5.9). The participants using such tools demonstrated the ability to create and store longer, more complex and far more unique password. They were also able to manage larger sets of user accounts, reusing identical passwords far less than those participants with no password manager tools.

One particular group from a specific demography, namely the Information Security sector, exhibited far better password usage and management behaviours. This particular result was not unexpected but reiterates the fact that knowing and clearly understanding security threats around poor password management will encourage users to implement a more secure approach to the management of their passwords.

Overall, the results indicated that South African users are not excluded from problems of managing usernames and passwords for their system accounts. They inevitably incorporate poor methods of password management practices and are seemingly not aided by their corporations or institutions in curtailing such poor and even risky behaviour. The knowledge necessary for improving this behaviour is understood, but is unfortunately not carried out as part of their password management strategy.

6.3 Summary of Contributions

This study has shown that South African computer users are comparable to other users around the world concerning their password management and usage habits.

The participants generally use weak password management methodologies and poor habits in their personal capacity as well as in their organisation or institution. Password reuse is an extremely common occurrence and is caused by users' needs to remember passwords for a large number of user accounts.

The organisations and institutions are implementing password policies, but these policies are apparently not improving users' password habits. They are, in some cases, actually inhibiting the users. These policies are possibly less restrictive than some of the users' personal account authentication systems.

Multi-Factor technologies are not being adopted by many of the participants' corporations or institutions. These technologies provide an enhancement to password-based authentication and because of this, users should be trained and made aware of the critical importance of applying these technologies.

There is a significant lack of security awareness training being provided to the participants. This training should be provided, not only as an introduction to password security, but also as a ongoing service to refresh the users' security knowledge as well provide awareness of new and prevalent security threats.

Password management software tools provide users with the ability to significantly improve their password management practices. These tools can be used to store credentials and generate unique, random and secure passwords for all of the users' accounts.

6.4 Further Research

The slow adoption rate or lack of multi-factor authentication in organisations and institutions is an interesting finding in this study. There are likely a number of reasons for this including cost, logistic problems or complexity. Further investigation into this finding could assist technology vendors to address this problem more specifically.

The use of password managers was not a common finding in this study even while it is clear that these tools improve the security level of passwords and generate unique passwords

for each of a users' accounts. An examination into the usability and confidence users have in these tools could accelerate the adoption rate.

There is an undeniable necessity for corporations and institutions to implement password policies on their computer systems. Users have indicated that these policies are more of a hindrance than an aid to managing their passwords. An investigation of the current password policies from a user experience and security requirement perspective would likely assist in the development of improved password policy implementation. This could also lead to the design of a common framework for creating such policies.

There is a need to identify why security awareness training is not being provided on a regularly basis to computer users. Organisations and institutions must be required to provide their users with information about protecting their user credentials and why it is important. A study into the security awareness training policies within organisations could certainly provide insight into the benefits and effectiveness of security training.

References

Adams, A. and Sasse, M. A. *Users are not the enemy. Communications of the ACM*, 42(12):40–46, 1999. doi:10.1145/322796.322806.

Albanesius, C. *Sony LulzSec Hack: What You Need to Know — News & Opinion — PCMag.com*. June 2011. Online.
Retrieved from `http://www.pcmag.com/article2/0,2817,2386362,00.asp`
Retrieved on 6 December 2013.

Albrechtsen, E. *A qualitative study of users' view on information security. Computers & Security*, 26(4):276–289, 2007. doi:10.1016/j.cose.2006.11.004.

AlFayyadh, B., Thorsheim, P., Jøsang, A., and Klevjer, H. *Improving usability of password management with standardized password policies.* In *7eme Conférence sur la Sécurité des Architectures Réseaux et Systemes d'Information (7th Conference on Network and Information Systems Security)(SAR-SSI 2012)*, pages 38–45. 2012.

Aussel, J.-D. *Smart cards and digital security.* In *Computer Network Security*, pages 42–56. Springer Berlin Heidelberg, 2007. ISBN 978-3-540-73985-2. doi:10.1007/978-3-540-73986-9_4.

Avoine, G., Junod, P., and Oechslin, P. *Characterization and Improvement of Time-Memory Trade-Off Based on Perfect Tables. ACM Transactions on Information and System Security*, 11(4):17:1–17:22, 2008. doi:10.1145/1380564.1380565.

Badra, M., El-Sawda, S., and Hajjeh, I. *Phishing attacks and solutions.* In *Proceedings of the 3rd international conference on Mobile multimedia communications*, page 42. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, 2007. ISBN 978-963-06-2670-5.

Baker, L. B. and Finkle, J. *Sony PlayStation suffers massive data breach -Reuters.* April 2011. Online.

Retrieved from `http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426`
Retrieved on 3 Decemeber 2013.

Berghel, H., Carpinter, J., and Jo, J.-Y. *Phish phactors: Offensive and defensive strategies. Advances in Computers*, 70:223–268, 2007.

Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., and Elliott, S. J. *Privacy preserving multi-factor authentication with biometrics. Journal of Computer Security*, 15(5):529–560, 2007.

Bidgoli, H. *The Internet Encyclopedia.* The Internet Encyclopedia. John Wiley & Sons, 2004. ISBN 0471222038.

Bishop, M. and Klein, D. V. *Improving system security via proactive password checking. Computers & Security*, 14(3):233–249, 1995. doi:10.1016/0167-4048(95)00003-Q.

Boatwright, M. and Luo, X. *What do we know about biometrics authentication?* In *Proceedings of the 4th annual conference on Information security curriculum development*, pages 31:1–31:5. ACM, New York, NY, USA, 2007. ISBN 978-1-59593-909-8. doi:10.1145/1409908.1409942.

Brand, S. and Makey, J. D. *Department of Defense password management guideline. CSC-STD-002–85, USA Government*, 1985.
Retrieved from `http://www.fas.org/irp/nsa/rainbow/std002.htm`
Retrieved on 1 December 2013.

Brodkin, J. *The secret to online safety: Lies, random characters, and a password manager — Ars Technica.* June 2013. Online.
Retrieved from `http://arstechnica.com/information-technology/2013/06/the-secret-to-online-safety-lies-random-characters-and-a-password-manager/`
Retrieved on 29 October 2013.

Brown, A. S., Bracken, E., Zoccoli, S., and Douglas, K. *Generating and remembering passwords. Applied Cognitive Psychology*, 18(6):641–651, 2004. doi:10.1002/acp.1014.

Brown, K. *The Dangers of Weak Hashes. SANS Institute InfoSec Reading Room*, pages 1–22, November 2013.
Retrieved from `http://www.sans.org/reading-room/whitepapers/authentication/dangers-weak-hashes-34412`

Bryant, K. and Campbell, J. *User Behaviours Associated with Password Security and Management. Australasian Journal of Information Systems*, 14(1), 2006.
Retrieved from `http://dl.acs.org.au/index.php/ajis/article/view/9`

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. *Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. MIS Quarterly*, 34(3):523–548, 2010.

Burnett, M. and Kleiman, D. *Perfect Passwords: Selection, Protection, Authentication.* Syngress Publishing, Rockland, Massachusetts, United States, 2006. ISBN 1597490415.

Carnegie Mellon University CERT. *CERT Incident Note IN-98.03: Password Cracking Activity.* July 1998. Online.
Retrieved from `http://www.cert.org/incident_notes/IN-98.03.html`
Retrieved on 1 October 2013.

Chen, B. X. *Apple Stops Password Resets Over the Phone - NYTimes.com.* August 2012. Online.
Retrieved from `http://bits.blogs.nytimes.com/2012/08/08/apple-stops-password-resets-over-the-phone/?_r=0`
Retrieved on 9 December 2013.

Chiasson, S., van Oorschot, P. C., and Biddle, R. *A usability study and critique of two password managers.* In *Proceedings of the 15th conference on USENIX Security Symposium - Volume 15*, pages 1–16. USENIX Association, Berkeley, CA, USA, 2006.

Chinitz, J. *Single Sign-On: Is It Really Possible? Information Systems Security*, 9(3):1–14, 2000.

Cluley, G. *YouPorn passwords available for download, thousands of users exposed — Naked Security.* February 2012. Online.
Retrieved from `http://nakedsecurity.sophos.com/2012/02/22/youporn-password-download/`
Retrieved on 7 December 2013.

Cooper, M. H. *Information security training: lessons learned along the trail.* In *Proceedings of the 36th annual ACM SIGUCCS fall conference: moving mountains, blazing trails*, pages 207–212. ACM, New York, NY, USA, 2008. ISBN 978-1-60558-074-6. doi: 10.1145/1449956.1450020.

Cubrilovic, N. *RockYou Hack: From Bad To Worse — TechCrunch*. January 2009. Online.
Retrieved from `http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/`
Retrieved on 7 December 2013.

Das, R. *An introduction to biometrics. Military Technology*, 29(7):20–27, 2005.

Desman, M. B. *The ten commandments of information security awareness training. Information Systems Security*, 11(6):39–44, 2003.

Didymus, J. T. *YouPorn security breach exposes thousands of usernames, emails*. February 2012. Online.
Retrieved from `http://digitaljournal.com/article/320123`
Retrieved on 7 December 2013.

Duggan, G. B., John-on, H., and Grawemeyer, B. *Rational security: Modelling everyday password use. International Journal of Human-Computer Studies*, 70(6):415–431, 2012. doi:10.1016/j.ijhcs.2012.02.008.

Eminağaoğlu, M., Uçar, E., and Eren, c. *The Positive Outcomes of Information Security Awareness Training in Companies - A Case Study. Information Security Tech. Report*, 14(4):223–229, 2009. doi:10.1016/j.istr.2010.05.002.

Feldmeier, D. C. and Karn, P. R. *Unix password security-ten years later*. In *Advances in Cryptology—CRYPTO'89 Proceedings*, pages 44–63. Springer, 1990.

Fitzgerald, D. *Yahoo Investigates Password Breach - WSJ.com*. July 2012. Online.
Retrieved from `http://online.wsj.com/news/articles/SB10001424052702304373804577522613740363638`
Retrieved on 7 December 2013.

Florencio, D. and Herley, C. *A Large-scale Study of Web Password Habits*. In *Proceedings of the 16th International Conference on World Wide Web*, pages 657–666. ACM, New York, NY, USA, 2007. ISBN 978-1-59593-654-7. doi:10.1145/1242572.1242661.

Florencio, D., Herley, C., and Coskun, B. *Do strong web passwords accomplish anything. HOTSEC'07 Proceedings of the 2nd USENIX workshop on Hot topics in security*, pages 10:1–10:6, 2007.

Fontana, J. *Stolen passwords re-used to attack Best Buy accounts — ZDNet*. July 2012. Online.
Retrieved from `http://www.zdnet.com/stolen-passwords-re-used-to-attack-best-buy-acc`
Retrieved on 10 August 2013.

Furnell, S. M., Dowland, P. S., Illingworth, H. M., and Reynolds, P. L. *Authentication and Supervision: A Survey of User Attitudes. Computers & Security*, 19(6):529–539, 2000. doi:10.1016/S0167-4048(00)06027-2.

Gaw, S. and Felten, E. W. *Password management strategies for online accounts*. In *the second symposium*, pages 44–55. ACM Press, New York, New York, USA, 2006. ISBN 1595934480. doi:10.1145/1143120.1143127.

Gibson, S. and Laporte, L. *Security Now! Transcript of Episode #256*. The TWiT.tv Netcast Network, June 2010.
Retrieved from `https://www.grc.com/sn/sn-256.htm`

Glasow, P. A. *Fundamentals of Survey Research Methodology*. Technical report, The MITRE Corporation, Bedford, MA, United States, 2005.

Gold, S. *Cracking passwords. Network Security*, 2010(8):4–7, 2010. doi:http://dx.doi.org/10.1016/S1353-4858(10)70103-3.

Goodin, D. *Anatomy of a hack: How crackers ransack passwords like "qeadzcwrsfxv1331" — Ars Technica*. May 2013a. Online.
Retrieved from `http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/`
Retrieved on 12 October 2013.

Goodin, D. *How an epic blunder by Adobe could strengthen hand of password crackers — Ars Technica*. November 2013b. Online.
Retrieved from `http://arstechnica.com/security/2013/11/how-an-epic-blunder-by-adobe-could-strengthen-hand-of-password-crackers/`
Retrieved on 7 December 2013.

Granger, S. *The Simplest Security: A Guide To Better Password Practices — Symantec Connect Community*. January 2002. Online.
Retrieved from `http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices`
Retrieved on 2 November 2013.

Guzel, B. *Understanding Hash Functions and Keeping Passwords Safe — Nettuts+.* June 2012. Online.
Retrieved from `http://net.tutsplus.com/tutorials/php/understanding-hash-functions-and-keeping-passwords-safe/`
Retrieved on 12 December 2013.

Haller, N., Metz, C., Nesser, P., and Straw, M. *RFC 2289 A one-time password system.* Technical report, The Internet Engineering Task Force (IETF), 1996.

Halsey, M. *How Secure is Your Password? — Ghacks.* April 2012. Online.
Retrieved from `http://www.ghacks.net/2012/04/07/how-secure-is-your-password/`
Retrieved on 24 January 2014.

Hart, D. *Attitudes and practices of students towards password security. Journal of Computing Sciences in Colleges*, 23(5):169–174, May 2008.
Retrieved from `http://dl.acm.org/citation.cfm?id=1352627.1352653`

Hayden, M. *Crank Up App Security With Multi-Factor Authentication - Rackspace Developer Center.* March 2013. Online.
Retrieved from `http://developer.rackspace.com/blog/crank-up-app-security-with-multi-factor-authentication.html`
Retrieved on 13 December 2013.

Herath, T. and Rao, H. R. *Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems*, 47(2):154–165, 2009. doi:10.1016/j.dss.2009.02.005.

Herley, C., Oorschot, P. C., and Patrick, A. S. *Passwords: If We'Re So Smart, Why Are We Still Using Them?* In **Dingledine, R. and Golle, P.**, editors, *Financial Cryptography and Data Security*, pages 230–237. Springer-Verlag, Berlin, Heidelberg, 2009. ISBN 978-3-642-03548-7. doi:10.1007/978-3-642-03549-4_14.

Honan, M. *How Apple and Amazon Security Flaws Led to My Epic Hacking — Gadget Lab — Wired.com.* June 2012. Online.
Retrieved from `http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/`
Retrieved on 1 December 2013.

Howard, A. and Hu, Y. *An Approach for Detecting Malicious Keyloggers.* In *Proceedings of the 2012 Information Security Curriculum Development Conference*,

pages 53–56. ACM, New York, NY, USA, 2012. ISBN 978-1-4503-1538-8. doi: 10.1145/2390317.2390326.

Hunt, T. *Troy Hunt: A brief Sony password analysis.* June 2011. Online.
Retrieved from `http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html`
Retrieved on 20 October 2013.

Hunt, T. *Troy Hunt: What do Sony and Yahoo! have in common? Passwords!* June 2012. Online.
Retrieved from `http://www.troyhunt.com/2012/07/what-do-sony-and-yahoo-have-in-common.html`
Retrieved on 10 August 2013.

Inglesant, P. G. and Sasse, M. A. *The true cost of unusable password policies: password use in the wild.* In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 383–392. ACM, New York, NY, USA, 2010. ISBN 978-1-60558-929-9. doi:10.1145/1753326.1753384.

Ives, B., Walsh, K. R., and Schneider, H. *The domino effect of password reuse. Communications of the ACM*, 47(4):75–78, April 2004. doi:10.1145/975817.975820.

Kahate, S. A. *Keylogger Use for Security of A Personal Computer. International Journal of Engineering*, 2(1), 2013.

Kale, E. *Adobe hack update: Not 3 million. Not 38 million. 130 million accounts. — TG Daily.* November 2013. Online.
Retrieved from `http://www.tgdaily.com/security-brief/81284-adobe-hack-update-not-3-million-not-38-million-130-million-accounts`
Retrieved on 7 December 2013.

Kaliski, B. *RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0. tools.ietf.org*, September 2000.
Retrieved on 12 December 2013.

Kamp, P.-H. *LinkedIn Password Leak: Salt Their Hide. Queue*, 10(6):20:20–20:22, 2012. doi:10.1145/2246036.2254400.

Kaplan, D. *Yahoo confirms breach, passwords appear not encrypted - SC Magazine.* July 2012. Online.
Retrieved from `http://www.scmagazine.com/yahoo-confirms-breach-passwords-appear-not`

article/250002/
Retrieved on 7 December 2013.

Karole, A., Saxena, N., and Christin, N. *A comparative usability evaluation of traditional password managers.* In *Proceedings of the 13th international conference on Information security and cryptology*, pages 233–251. Springer-Verlag, Berlin, Heidelberg, 2011. ISBN 978-3-642-24208-3.

Kedem, G. and Ishihara, Y. *Brute force attack on UNIX passwords with SIMD computer.* In *In Proceedings of The 8th USENIX Security Symposium*, pages 93–98. 1999.

Kelly, S. M. *The 30 Most Popular Passwords Stolen From LinkedIn [INFOGRAPHIC].* June 2012. Online.
Retrieved from http://mashable.com/2012/06/08/linkedin-stolen-passwords-list/
Retrieved on 5 December 2013.

Khandelwal, T. *Passwords are not enough — Canadian Security.* September 2012. Online.
Retrieved from http://www.canadiansecuritymag.com/IT-Security/Editorial/Passwords-are-not-enough.html
Retrieved on 29 Ocotber 2013.

Kingsley-Hughes, A. *Cheap GPUs are rendering strong passwords useless — ZDNet.* June 2011. Online.
Retrieved from http://www.zdnet.com/blog/hardware/cheap-gpus-are-rendering-strong-passwords-useless/13125
Retrieved on 5 November 2013.

Kitten, T. *LinkedIn: Hashed Passwords Breached - GovInfoSecurity.* June 2012. Online.
Retrieved from http://www.govinfosecurity.com/linkedin-confirms-password-breach-a-4rf=2012-06-07-eg
Retrieved on 5 December 2013.

Klein, D. V. *Foiling the cracker: A survey of, and improvements to, password security.* In *Multiple values selected*, pages 5–14. 1990.
Retrieved from http://cs.gmu.edu/~csnow/library/unix/Klein_passwd.pdf
Retrieved on 5 November 2013.

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., and Egelman, S. *Of passwords and people: measuring the effect*

of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2595–2604. ACM, New York, NY, USA, 2011. ISBN 978-1-4503-0228-9. doi:10.1145/1978942.1979321.

Krebs, B. *Adobe To Announce Source Code, Customer Data Breach — Krebs on Security*. October 2013. Online.
Retrieved from `http://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/`
Retrieved on 7 December 2013.

Kuhn, D. R., Hu, V. C., Polk, W. T., and Chang, S.-J. *SP 800-32. Introduction to Public Key Technology and the Federal PKI Infrastructure*. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2001.

Lehohla, P. *Census 2011 Census in brief - Statistics South Africa. ISBN 978-0-621-41388-5*, pages 1–107, October 2012.
Retrieved from `http://www.statssa.gov.za/census2011/Products/Census_2011_Census_in_brief.pdf`

Leyden, J. *RockYou password snafu exposes webmail accounts - The Register*. December 2009. Online.
Retrieved from `http://www.theregister.co.uk/2009/12/16/rockyou_password_snafu/`
Retrieved on 7 December 2013.

Leyden, J. *RockYou hack reveals easy-to-crack passwords - The Register*. January 2010. Online.
Retrieved from `http://www.theregister.co.uk/2010/01/21/lame_passwords_exposed_by_rockyou_hack/`
Retrieved on 7 December 2013.

Mannan, M. and van Oorschot, P. C. *Passwords for both Mobile and Desktop Computers: ObPwd for Firefox and Android. USENIX;login*, 37(4), August 2012.

Marechal, S. *Advances in password cracking. Journal in computer virology*, 4(1):73–81, 2008. doi:10.1007/s11416-007-0064-y.

Mattila, A. and Mattila, M. *What is the Effect of Product Attributes on Public-Key Infrastructure adoption? The IPSI BgD Transactions on Internet Research*, 2(1):16, January 2006. ISSN 1820-4503.

Matyás Jr., V. and Riha, Z. *Toward Reliable User Authentication Through Biometrics. Security & Privacy, IEEE*, 1(3):45–49, 2003. doi:10.1109/MSECP.2003.1203221.

Merkle, R. *A fast software one-way hash function. Journal of Cryptology*, 3(1):43–58, 1990. doi:10.1007/BF00203968.

Mirkovic, J., Hussain, A., Wilson, B., Fahmy, S., Reiher, P., Thomas, R., Yao, W.-M., and Schwab, S. *A user-centric metric for denial-of-service measurement.* In *Experimental computer science on Experimental computer science*, pages 7–7. USENIX Association, Berkeley, CA, USA, 2007.

Morris, R. and Thompson, K. *Password Security: A Case History. Communications of the ACM*, 22(11):594–597, 1979. doi:10.1145/359168.359172.

Moshe, S. B. *Password Entropy — shay.co blog.* August 2011. Online.
Retrieved from `http://blog.shay.co/password-entropy/`
Retrieved on 12 November 2013.

Needham, R. M. and Schroeder, M. D. *Using Encryption for Authentication in Large Networks of Computers. Communications of the ACM*, 21(12):993–999, 1978. doi:10.1145/359657.359659.

Notoatmodjo, G. and Thomborson, C. *Passwords and perceptions.* In *Proceedings of the Seventh Australasian Conference on Information Security*, pages 71–78. Australian Computer Society, Inc., Darlinghurst, Australia, Australia, 2009. ISBN 978-1-920682-79-8.

O'Dell, J. *860,000 Accounts Leaked from Anonymous STRATFOR hack.* January 2012. Online.
Retrieved from `http://readersupportednews.org/news-section2/335-156/9229-860000-accounts-leaked-from-anonymous-stratfor-hack`
Retrieved on 7 December 2013.

O'Gorman, L. *Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE*, 91(12):2021–2040, 2003. doi:10.1109/JPROC.2003.819611.

Olivarez-Giles, N. *Amazon Quietly Closes Security Hole After Journalist's Devastating Hack — Gadget Lab — Wired.com.* July 2012. Online.
Retrieved from `http://www.wired.com/gadgetlab/2012/08/amazon-changes-policy-wont-add-new-credit-cards-to-accounts-over-the-phone/`
Retrieved on 9 December 2013.

Orgill, G. L., Romney, G. W., Bailey, M. G., and Orgill, P. M. *The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems.* In *Proceedings of the 5th Conference on Information Technology Education*, pages 177–181. ACM, New York, NY, USA, 2004. ISBN 1-58113-936-5. doi:10.1145/1029533.1029577.

Pashalidis, A. and Mitchell, C. J. *A Taxonomy of Single Sign-on Systems.* In *Proceedings of the 8th Australasian Conference on Information Security and Privacy*, pages 249–264. Springer-Verlag, Berlin, Heidelberg, 2003. ISBN 3-540-40515-1. doi:10.1007/3-540-45067-X_22.

Peckham, M. *Everything You Need to Know About the Sony PlayStation Network Fiasco — TIME.com.* April 2011. Online.
Retrieved from `http://techland.time.com/2011/04/27/everything-you-need-to-know-about-the-sony-playstation-network-fiasco/`
Retrieved on 28 November 2013.

Peltier, T. R. *Social Engineering: Concepts and Solutions. Information Systems Security*, 15(5):13–21, 2006. doi:10.1201/1079.07366981/45802.33.8.20060201/91956.1.

Percival, C. *Stronger key derivation via sequential memory-hard functions. Self-published*, 2009.
Retrieved from `http://www.tarsnap.com/scrypt/scrypt.pdf`
Retrieved on 20 November 2013.

Perlroth, N. *Hackers Breach the Web Site of Stratfor Global Intelligence - NYTimes.com.* December 2011. Online.
Retrieved from `http://www.nytimes.com/2011/12/26/technology/hackers-breach-the-web-site-of-stratfor-global-intelligence.html?_r=0`
Retrieved on 7 December 2013.

Pilar, D. R., Jaeger, A., Gomes, C. F. A., and Stein, L. M. *Passwords Usage and Human Memory Limitations: A Survey across Age and Educational Background. PLoS ONE*, 7(12):e51067, December 2012. doi:10.1371/journal.pone.0051067.t006.

Pinkas, B. and Sander, T. *Securing passwords against dictionary attacks.* In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 161–170. ACM, New York, NY, USA, 2002. ISBN 1-58113-612-9. doi:10.1145/586110.586133.

Proctor, R. W., Lien, M.-C., Vu, K.-P. L., Schultz, E. E., and Salvendy, G. *Improving computer security for authentication of users: Influence of proactive password restrictions. Behavior Research Methods, Instruments, & Computers*, 34(2):163–169, 2002.

Provos, N. and Mazieres, D. *A Future-Adaptable Password Scheme.* In *USENIX Annual Technical Conference, FREENIX Track*, pages 81–91. 1999.

Ragan, S. *Follow-up analysis of the Stratfor password list (Part 1).* January 2012. Online.
Retrieved from `http://www.thetechherald.com/articles/Follow-up-analysis-of-the-Stratfor-password-list-(Part-1)`
Retrieved on 7 December 2013.

Raphael, J. R. *Gawker Hack Exposes Ridiculous Password Habits — PCWorld.* December 2010. Online.
Retrieved from `http://www.pcworld.com/article/213679/Gawker_Hack_Exposes_Ridiculous_Password_Habits.html`
Retrieved on 27 October 2013.

Rashid, F. Y. *Sony PlayStation Network Data Breach Compromises 77 Million User Accounts.* April 2011. Online.
Retrieved from `http://www.eweek.com/c/a/Security/Sony-PlayStation-Network-Data-Breach-Compromises-77-Million-User-Accounts-208028/`
Retrieved on 4 December 2013.

Rashid, F. Y. *Analysis of Stratfor Site Breach Reveals Weak Passwords, Poor Enforcement.* January 2012. Online.
Retrieved from `http://www.eweek.com/c/a/Security/Analysis-of-Stratfor-Site-Breach-Reveals-Weak-Passwords-Poor-Enforcement-719464/`
Retrieved on 7 December 2013.

Riley, S. *Password security: What users know and what they actually do. Usability News*, 8(1), 2006.
Retrieved from `http://psychology.wichita.edu/surl/usabilitynews/81/pdf/Usability%20News%2081%20-%20Riley.pdf`

Roberts, P. *New 25 GPU Monster Devours Passwords In Seconds — The Security Ledger.* December 2012. Online.
Retrieved from `https://securityledger.com/2012/12/`

new-25-gpu-monster-devours-passwords-in-seconds/
Retrieved on 12 December 2013.

Saltzer, J. H. and Schroeder, M. D. *The protection of information in computer systems. Proceedings of the IEEE*, 63(9):1278–1308, 1975. doi:10.1109/PROC.1975.9939.

Scarfone, K. and Souppaya, M. *Guide to enterprise password management (draft)*, volume 800 of *Recommendations of the National Institute of Standards and Technology*. Books LLC, September 2011. ISBN 9781234114961.

Schneier, B. *The Blowfish encryption algorithm. Dr Dobb's Journal-Software Tools for the Professional Programmer*, 19(4):38–43, 1994.

Schneier, B. *Schneier on Security: Changing Passwords*. November 2010. Online.
Retrieved from https://www.schneier.com/blog/archives/2010/11/changing_passwo.html
Retrieved on 20 October 2013.

Schroeder, S. *YouPorn User Emails and Passwords Exposed*. February 2012. Online.
Retrieved from http://mashable.com/2012/02/23/youporn-hack/
Retrieved on 7 December 2013.

Schwartz, M. J. *Sony Data Breach Cleanup To Cost $171 Million - InformationWeek*. May 2011. Online.
Retrieved from http://www.informationweek.com/attacks/sony-data-breach-cleanup-to-cost-$171-million/d/d-id/1097898?
Retrieved on 6 December 2013.

Shaw, J. *Dealing with encryption. Network Security*, 2013(11):8–11, 2013. doi:10.1016/S1353-4858(13)70120-X.

Shay, R. and Bertino, E. *A comprehensive simulation tool for the analysis of password policies. International Journal of Information Security*, 8(4):275–289, 2009. doi:10.1007/s10207-009-0084-3.

Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., and Cranor, L. F. *Encountering stronger password requirements: user attitudes and behaviors*. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, pages 2:1–2:20. ACM, New York, NY, USA, 2010. ISBN 978-1-4503-0264-7. doi:10.1145/1837110.1837113.

Siciliano, R. *Is a Password Enough? A Closer Look at Authentication.* August 2012. Online.
Retrieved from `http://www.infosecisland.com/blogview/22096-Is-a-Password-Enough-A-Closer-Look-at-Authentication.html`
Retrieved on 2 November 2013.

Siegler, M. G. *One Of The 32 Million With A RockYou Account? You May Want To Change All Your Passwords. Like Now. — TechCrunch.* December 2009. Online.
Retrieved from `http://techcrunch.com/2009/12/14/rockyou-hacked/`
Retrieved on 7 December 2013.

Snyder, R. *Ethical hacking and password cracking: a pattern for individualized security exercises.* In *Proceedings of the 3rd annual conference on Information security curriculum development*, pages 13–18. ACM, New York, NY, USA, 2006. ISBN 1-59593-437-5. doi:10.1145/1231047.1231051.

Summers, W. C. and Bosworth, E. *Password policy: the good, the bad, and the ugly. Winter International Symposium on Information and Communication Technologies 2004*, pages 1–6, 2004.

Tamil, E. M., Othman, A. H., Abidin, S. A. Z., Idris, M. Y. I., and Zakaria, O. *Password Practices: A Study on Attitudes towards Password Usage among Undergraduate Students in Klang Valley, Malaysia. Journal of Advancement of Science & Arts*, 3:37–42, 2007.
Retrieved from `http://www.ucsi.edu.my/cervie/ijasa/volume3/pdf/ac4.pdf`

Teat, C. and Peltsverger, S. *The Security of Cryptographic Hashes.* In *Proceedings of the 49th Annual Southeast Regional Conference*, pages 103–108. ACM, New York, NY, USA, 2011. ISBN 978-1-4503-0686-7. doi:10.1145/2016039.2016072.

United States General Accounting Office. *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology.* Technical Report GAO-01-277, United States General Accounting Office, February 2001.

Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., and Cranor, L. F. *How does your password measure up? the effect of strength meters on password creation.* In *Proceedings of the 21st USENIX conference on Security symposium*, pages 5–5. USENIX Association, Berkeley, CA, USA, 2012.

Wagner, D. and Goldberg, I. *Proofs of Security for the Unix Password Hashing Algorithm.* In *Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, pages 560–572. Springer-Verlag, London, UK, UK, 2000. ISBN 3-540-41404-5.

Walton, Z. *Yahoo Password Breach Is Worse Than Originally Thought — WebProNews.* July 2012. Online.
Retrieved from `http://www.webpronews.com/yahoo-password-breach-is-worse-than-origin`
Retrieved on 7 December 2013.

Weirich, D. and Sasse, M. A. *Pretty good persuasion: a first step towards effective password security in the real world.* In *Proceedings of the 2001 workshop on New security paradigms*, pages 137–143. ACM, New York, NY, USA, 2001. ISBN 1-58113-457-6. doi: 10.1145/508171.508195.

Wiberg, K. *How much entropy in that password? — Karl Wiberg.* August 2011. Online.
Retrieved from `https://subrabbit.wordpress.com/2011/08/26/how-much-entropy-in-that-password/`
Retrieved on 12 November 2013.

Wilkes, M. V. *Time Sharing Computer Systems.* Elsevier Science Inc., New York, NY, USA, 1975. ISBN 0444195254.

Williams, B. L. *Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2. 0, and AUP V5. 0.* Auerbach Pub, 2013.

Wilson, M. and Hash, J. *SP 800-50. Building an Information Technology Security Awareness and Training Program. NIST Special Publication*, 800:50, 2003.

Wisniewski, C. *HBGary Federal hacked and exposed by Anonymous — Naked Security.* February 2011. Online.
Retrieved from `http://nakedsecurity.sophos.com/2011/02/07/hbgary-federal-hacked-and-exposed-by-anonymous/`
Retrieved on 15 January 2014.

Wood, C. C. and Shield, I. *Information Security Policies Made Easy, Version 10.* Information Shield, Inc., 2008. ISBN 1881585131, 9781881585138.
Retrieved from `http://www.scribd.com/doc/24237390/Information-Security-Policy-Made-Easy-ISME-v10-Complete`

Wylder, J. O. *Improving security from the ground up. Information Systems Security*, 11(6):29–38, 2003.

Yan, J. J. *A note on proactive password checking.* In *Proceedings of the 2001 workshop on New security paradigms*, pages 127–135. ACM, New York, NY, USA, 2001. ISBN 1-58113-457-6. doi:10.1145/508171.508194.

Yin, S. *YouPorn Data Breach Exposes Usernames, Emails.* February 2012. Online. Retrieved from `http://securitywatch.pcmag.com/none/294477-youporn-data-breach-exposes-usernames-emails` Retrieved on 7 December 2013.

Zhang, J., Luo, X., Akkaladevi, S., and Ziegelmayer, J. *Improving multiple-password recall: an empirical study. European Journal of Information Systems*, 18(2):165–176, March 2009. doi:10.1057/ejis.2009.9.

Zviran, M. and Haga, W. J. *Password security: an empirical study. Journal of Management Information Systems*, 15:161–186, 1999.

Appendix A

Survey Disclaimer and Questions

Survey Disclaimer

Rhodes University: Research study on user experience with accounts and password management.

The purpose of this research project is to determine the password usage and habits of internet users. This is a research project being conducted by Brandon Friedman, a Computer Science post-graduate student at Rhodes University.

Your participation in this research study is voluntary.This survey is for South African residents only.

The procedure involves completing an online survey that will take approximately 10 to 15 minutes. Your responses will be confidential and we do not collect identifying information such as your name, email address or the organisation/institution you currently a member of. The survey questions will be about your experience with user account and password at your organisation/institution and in your private capacity.

Answering the questions honestly and completely is important so that the results of the research are accurate.

All data is stored in a password protected electronic format. To help protect your confidentiality, the surveys will not contain information that will personally identify you. The results of this study will be used for scholarly purposes only and may be shared with Rhodes University representatives.

If you have any questions about the research study, please contact g12F7027 [at] campus.ru.ac.za. This research has been reviewed according to Rhodes University Ethics procedures for research involving human subjects.

ELECTRONIC CONSENT:

Clicking on the "next" button below indicates that:

- you have read the above information
- you voluntarily agree to participate

There are 61 questions in this survey

Survey Questions

Demographics

The section has questions regarding information about you. Please complete all questions to the best of your ability.

[**Q0001**] Please select your location:

Please choose only one of the following:

- Gauteng
- Eastern Cape
- Free State
- KwaZulu-Natal
- Limpopo
- Mpumalanga
- Northern Cape
- Western Cape

- North West

[**Q0002**] Please specify your age group:

Please choose only one of the following:

- 6 to 12 years old
- 13 to 18 years old
- 19 to 25 years old
- 26 to 35 years old
- 36 to 45 years old
- 46 to 55 years old
- 55+ years old

[**Q0003**] Please select your gender:

Please choose only one of the following:

- Female
- Male

[**Q0004**] Please select your racial group:

Please choose only one of the following:

- African
- Asian
- Coloured
- Indian
- White

[**Q0005**] Please indicate your annual income:

Please choose only one of the following:

- R0 to R100 000 per year
- R100 000 to R200 000 per year
- R200 000 to R300 000 per year
- R300 000 to R400 000 per year
- R400 000 to R500 000 per year
- R500 000 to R600 000 per year
- R600 000 to R700 000 per year
- R700 000 to R800 000 per year
- R800 000+ per year

[**Q0006**] Please select the industry in which you are employed or studying toward:

Please choose only one of the following:

- Academic/Education
- Banking/Investment and Finance
- Engineering Government
- Health and Fitness
- Human Resources
- Information Technology
- Insurance
- Legal
- Manufacturing

- Property
- Retail
- Safety And Security
- Sales and Marketing
- Telecommunications
- Travel
- Other

[**Q0007**] Please select your current employment or professional status:

Please choose only one of the following:

- Employed
- Self-Employed
- Part-time Employed
- A Student
- Retired
- Other

[**Q0008**] Please select all the online social networking sites with which you have an account:

Please choose all that apply:

- Facebook
- Twitter
- LinkedIn
- Google Plus+

- MySpace
- Pinterest
- Youtube
- Flickr
- Other

[**Q0009**] Please select all the email websites or services with which you have an account:

Please choose all that apply:

- Gmail
- Hotmail
- Outlook.com
- Zoho
- Mail
- Yahoo
- Mail
- Email
- Provide by you ISP (Mweb, iBurst, Neotel, MTN etc)
- My own privately registered domain and email service
- Other

[**Q0010**] Please select any of the follow online services with which you have a username and password:

Please choose all that apply:

- Online Gaming (Xbox,Playstation Network, World of Warcraft etc)

- Online Gambling
- Online Auction/Classifieds websites (eBay, Bid or Buy,Gumtree etc)
- Blog Websites
- eCommerce Websites (Kalahari, Amazon etc)
- Other

[**Q0011**] Do you use the Internet banking services from your bank?

Please choose only one of the following:

- Yes
- No

[**Q0012**] Please select the bank whose internet banking services you use:

Only answer this question if the following conditions are met: Answer was 'Yes' at question '11 [**Q0011**]' (Do you use the Internet banking services from your bank?)

Please choose only one of the following:

- ABSA
- First National Bank
- Nedbank
- Standard Bank
- Other

[**Q0013**] Please indicate the level of concern you have for the security and privacy of your online account passwords?

Please choose only one of the following:

- I am not concerned about computer security.

- I am aware of the need to be computer security conscious but I trust the computer and IT staff to manage it for me.
- I am conscious of the need to protect my user account and I do so to the best of my ability.
- I am extremely conscious about computer security and I employ the maximum level of protection for my usernames and passwords.

Password Policies in your Organisation or Institution

This section has questions regarding the password policies and rules at your organisation/ institution.

[**Q0014**] Have you ever been at an organisation or institution (including your current one) that requires you to adhere to a password policy?

Please choose only one of the following:

- Yes
- No

A password policy encourages and enforces users to follow a set of password rules. These rules would include regularly changing your password and using strong alpha-numberic (letters and numbers).

[**Q0015**] Does your organisation/institution require you to have a minimum password length?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '14 [**Q0014**]' (Have you ever been at an organisation or institution (including your current one) that requires you to adhere to a password policy?)

Please choose only one of the following:

- Yes
- No

The password that you select must be a certain number of characters long (i.e. minimum password length is 8 characters.)

[**Q0016**] What is the minimum number of characters you are allowed to use in your password?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '15 [**Q0015**]' (Does your organisation/institution require you to have a minimum password length?)

Please choose only one of the following:

- 1 to 4 characters
- 5 to 8 characters
- 9 to 12 characters
- 12 to 15 characters
- 15+ characters

[**Q0017**] Does your organisation/institution require you to change your password on a regular basis?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '14 [**Q0014**]' (Have you ever been at an organisation or institution (including your current one) that requires you to adhere to a password policy?)

Please choose only one of the following:

- Yes
- No

[**Q0018**] How often are you required to change your password?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '17 [**Q0017**]' (Does your organisation/institution require you to change your password on a regular basis?)

Please choose only one of the following:

- Weekly
- Bi-weekly
- Every 30 days
- Every 60 days
- Every 90 days
- Other

[**Q0019**] Does your organisation require you to have a password that contains alpha-numeric characters?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '14 [**Q0014**]' (Have you ever been at an organisation or institution (including your current one) that requires you to adhere to a password policy?)

Please choose only one of the following:

- Yes
- No

Password that are alpha-numeric contain numbers and letters e.g. 2jpc4tr

[**Q0020**] Does your organisation/institution enforce password history tracking and prevention?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '14 [**Q0014**]' (Have you ever been at an organisation or institution (including your current one) that requires you to adhere to a password policy?)

Please choose only one of the following:

- Yes
- No

Enforcing password history tracking will prevent the user from reusing an old password when your current password has expired. The old password may not be used again until a specified number of password changes have been completed.

[**Q0021**] Does your organisation/institution prevent you from using names and/or dictionary words for your password?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '14 [**Q0014**]' (Have you ever been at an organisation or institution (including your current one) that requires you to adhere to a password policy?)

Please choose only one of the following:

- Yes
- No

Examples of dictionary words would include common words such as "monkey", "apple" or "bicycle". (These words can be from any language.) Examples of names would include your name, your surname, names of places and/or your account username.

[**Q0022**] How many user accounts do you have to remember at your organisation or institution?

Please choose only one of the following:

- 1 to 5 user accounts
- 6 to 10 user accounts
- 11 to 15 user accounts
- 15+ user accounts

[**Q0023**] Do you ever re-use the same password on different accounts in your organisation/ institution?

Please choose only one of the following:

- Yes

- No

[**Q0024**] How do you remember your passwords for your accounts at your organisation/ institution?

Please choose only one of the following:

- Memorise all of the passwords.
- Re-use the same or similar passwords from other accounts.
- Write the passwords down somewhere (e.g. piece of paper or a notebook or spreadsheet).
- Use password management software.

[**Q0025**] Have you ever shared your account password(s) with anyone else in your organisation/institution including IT-Staff members?

Please choose only one of the following:

- Yes
- No

[**Q0026**] Do you know the password of anyone else in your organisation/institution?

Please choose only one of the following:

- Yes
- No

[**Q0027**] Does your organisation/institution employ the use of multi-factor or 2-step verification technology with your user account login process?

Please choose only one of the following:

- Yes
- No

Mulit-factor or 2-step verification is a technology that includes an additional means of account verification along with your username and password. Examples of this include: A one-time password that is SMS'd to you when verifying your account. A security token that provides you with a pin number to include in your login. A smard card/token that needs to be inserted into your computer in order to login.

[**Q0028**] Do you think the multi-factor technology provides additional security or it is more of anuisance/annoyance to your login process?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '27 [**Q0027**]' (Does your organisation/institution employ the use of multi-factor or 2-step verification technology with your user account login process?)

Please choose only one of the following:

- Additonal security
- Nuisance/annoyance
- Both of the above

[**Q0029**] Does your organisation provide security awareness training?

Please choose only one of the following:

- Yes
- No

Security awareness training provides staff/members of the organisation/instittutions with the knowledge on how to secure and protect their information and assets from computer criminals.

[**Q0030**] Please select the method(s) that are used to promote security awareness:

Only answer this question if the following conditions are met: Answer was 'Yes' at question '29 [Q0029]' (Does your organisation provide security awareness training?)

Please choose all that apply:

- Formal training upon joining the organisation/institution
- Periodic training sessions (refresher courses)
- Security Posters
- Email campaigns
- Intranet articles and/or blogs
- Other

[**Q0031**] Do you think it is necessary to have all the rules to control the way you create and use your passwords in your organisation/institution?

Please choose only one of the following:

- Yes
- No

[**Q0032**] If you don't feel it is necessary for password policies, please indicate why?

Only answer this question if the following conditions are met: Answer was 'No' at question '31 [**Q0031**]' (Do you think it is necessary to have all the rules to control the way you create and use your passwords in your organisation/institution?)

Please choose all that apply:

- Difficult passwords are hard to remember.
- What's the point? Nobody wants to steal my password.
- Changing passwords all the time is annoying.
- It is easier to use the same password on all my accounts.
- Other

Personal password management

In this section the questions will relate to your personal password usage and management. This will include all online or computer user account that are not related to work or educational purposes

[**Q0033**] How many private user accounts do you have that require a username and password to login?

Please choose only one of the following:

- 1 to 3 accounts
- 4 to 8 accounts
- 9 to 15 accounts
- 16 to 20 accounts
- 20+ accounts

Please include all of your online and computer accounts. For example: Facebook Twitter Email Internet banking Desktop or laptop user account

[**Q0034**] How do you remember your private user accounts and passwords for all of your online/computer credentials?

Please choose only one of the following:

- I try to memorise all of the usernames and passwords.
- In order to remember my username/password, I re-use the same username/password on most of my accounts.
- I write the usernames and passwords down somewhere (e.g. a piece of paper, a notebook or spreadsheet).
- I use password management software. I use my browser to store and manage my passwords.
- Other

[**Q0035**] Please select the password management software that you primarily use to manage your passwords:

Only answer this question if the following conditions are met: Answer was 'I use password management software.' at question '34 [**Q0034**]' (How do you remember your private user accounts and passwords for all of your online/computer credentials?)

Please choose only one of the following:

- 1Password
- LastPass
- KeePass
- Roboform
- STRIP
- SplashID
- Other

[**Q0036**] How often do you change the passwords of your personal accounts?

Please choose only one of the following:

- Once a week
- Once a month
- Every 3 to 6 months
- Every 6 to 12 months
- Longer than 12 months
- Never

[**Q0037**] Do you ever reuse the same password for different personal accounts?

Please choose only one of the following:

- Yes
- No

[**Q0038**] How often do you reuse the same password on different accounts?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '37 [**Q0037**]' (Do you ever reuse the same password for different personal accounts?)

Please choose only one of the following:

- All or most of my accounts use the same password.
- I use the same password on 8 or less accounts and then use another password on the next group of accounts.
- I use the same password on 3 or less accounts and then use another passoword on the next group of accounts.
- I use the same password on most of my accounts but a different password(s) on accounts I consider to be more important (and want to protect).

[**Q0039**] What is the average length (number of characters) you use for your personal account passwords?

Please choose only one of the following:

- 1 to 4 characters
- 5 to 8 characters
- 9 to 15 characters
- 16 to 20 characters
- 20+ characters
- Other

[**Q0040**] How many unique passwords do you use for your personal accounts?

Please choose only one of the following:

- 1 to 3 unique passwords
- 4 to 8 unique passwords
- 9 to 12 unique passwords
- 12 to 15 unique passwords
- 15+ unique passwords

You may have a group or pool of passwords that you commonly use when creating or registering a new user account.

[**Q0041**] Do you ever use personal information as your password or to form part of your password content?

Please choose only one of the following:

- Yes
- No Personal information may include some of the following examples:

Names of people or pets Birthday dates Telephone numbers Personal interests or hobbies

[**Q0042**] Please select the types of personal information that you have included in any of your personal passwords:

Only answer this question if the following conditions are met: Answer was 'Yes' at question '41 [**Q0041**]' (Do you ever use personal information as your password or to form part of your password content?)

Please choose all that apply:

- Special Number (Lucky number, ATM PIN number, ID Number etc)
- Special Dates (Birthdays, anniversary etc)
- Names of people (Family members, work colleagues, celebrities etc)
- Names of place (Place of birth, city of residence, places you have travelled to etc)
- Hobbies or interests (Sports, car you drive, favourite restaurant etc)

- Other

[Q0043] Do you use your ATM/bank card PIN number as password for any of your accounts?

Please choose only one of the following:

- Yes
- No

[Q0044] Please select the characters types that you use when creating your passwords:

Please choose only one of the following:

- Letters only
- Numbers only
- Letters and Numbers
- Letters, Numbers and Special Characters (e.g. !@#$%^&)
- Letters (Upper and lower-case) and Numbers
- Letters (Upper and lower-case) Numbers and Special Characters (e.g. !@#$%^&)

[Q0045] Have you ever shared your personal account credentials (username and password) with anyone (deliberately or accidentally)?

Please choose only one of the following:

- Yes
- No

[**Q0046**] Did you change the password after you had shared or discovered that it had been shared with someone else?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '45 [**Q0045**]' (Have you ever shared your personal account credentials (username and password) with anyone (deliberately or accidentally)?)

Please choose only one of the following:

- Yes
- No

[**Q0047**] Do you use dictionary words as your passwords (in any language)?

Please choose only one of the following:

- Yes
- No

[**Q0048**] Do you ever use multi-factor or 2-step verification for your personal account logins?

Please choose only one of the following:

- Yes
- No

Multi-factor or 2-step verification is a technology that provides an additional verification step when logging onto one of your online or computer accounts. This may include one of the following examples: An SMS with a one-time password when logging to your internet banking website or completing an internet banking transaction. An SMS from facebook or other social networking website when login on. Google Authenticator when you login to your Gmail account.

[**Q0049**] Do you feel that multi-factor authentication verification is a security enhancement or a nuisance when using your personal accounts?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '48 [**Q0048**]' (Do you ever use multi-factor or 2-step verification for your personal account logins?)

Please choose only one of the following:

- Security enhancement
- Nuisance
- Both of the above

[**Q0050**] How often do you forget the password to one of your personal accounts?

Please choose only one of the following:

- I rarely forget my passwords (I have to reset no more than one password per year)
- I seldom forget my passwords (I have to reset two to five passwords per year)
- I often forget my passwords (I have to reset six to fifteen passwords per year)
- I forget passwords very often (fifteen or more passwords per year)

[**Q0051**] Have you ever had to use a password retrieval or "Forgot Password?" facility for any of your online accounts?

Please choose only one of the following:

- Yes
- No

[**Q0052**] What was the process that allowed you to retrieve or reset your password?

Only answer this question if the following conditions are met: Answer was 'Yes' at question '51 [**Q0051**]' (Have you ever had to use a password retrieval or "Forgot Password?" facility for any of your online accounts?)

Please choose all that apply:

- The website emailed me my password and I was able to login again.
- The website emailed me a webpage link which I clicked on. I had to create a new password on the website I was directed to.
- I had to answer a number of security questions and then I was able to create a new password.
- The website emailed me a new temporary password and then I was able to login again.
- The website sent me webpage link to reset my password. I also received an SMS with a pin to verify the password reset.
- Other

[**Q0053**] Do you currently use any of the passwords below for you personal user accounts?

1. password
2. qwerty
3. 123456
4. 12345678
5. monkey
6. letmein
7. abc123
8. dragon
9. charlie
10. iloveyou

Please choose only one of the following:

- Yes

- No

[Q0054] Please select the password(s) from the list that you are using:

Only answer this question if the following conditions are met: Answer was 'Yes' at question '53 [Q0053]' (Do you currently use any of the passwords below for you personal user accounts? password qwerty 123456 12345678 monkey letmein abc123 dragon charlie iloveyou)

Please choose all that apply:

- password
- qwerty
- 123456
- 12345678
- monkey
- letmein
- abc123
- dragon
- charlie
- iloveyou

[Q0055] Do you think the passwords that you use for your personal accounts are strong and secure?

Please choose only one of the following:

- Yes
- No

Strong and secure passwords are not easily guessable by humans nor are they easy to "crack" by a computer program.

Security and Password ratings

The following selection includes questions about the importance of the websites you visit and your thoughts on password security strength.

[**Q0056**] Please rank, in order of importance, the account password you feel most needs to be kept secret (rank from most important to least important).

Please number each box in order of preference from 1 to 5

- Social networking website (Facebook, Twitter etc)
- Email website or service
- Internet banking
- Online gaming account
- eCommerce/retail websites (Kalahari, Amazon,eBay etc)

The list includes some of the most popular online services and websites on the internet. Even if you do NOT use all of these online facilities, please still order them in the order of importance you feel they should be in.

[**Q0057**] Please rank, in order of strength, the passwords listed (please order them from most/highest to least/lowest security):

Please number each box in order of preference from 1 to 5

- H0t3L9098
- Antelope2
- $#pL@n3tEARt4
- Apple
- Mustang10

[**Q0058**] Please rank, in order of similarity, which passwords (listed below) resemble the passwords that you use for your common user accounts (from most similar to least similar):

Please number each box in order of preference from 1 to 5

- H0t3L9098
- Antelope2
- $#pL@n3tEARt4
- Apple
- Mustang10

[**Q0059**] Please indicate which attributes you think contribute to increasing the strength of a password:

Please choose all that apply:

- The number of characters in the password
- Using letters and numbers
- Using personal related terms (such as your birth date, relatives name, favourite colour etc)
- Using special characters (e.g. $%#@!)
- Other

[**Q0060**] Do you feel that usernames and passwords are sufficient protection for your personal online accounts?

Please choose only one of the following:

- Yes
- No

[**Q0061**] What other types of technology do you feel would improve the security and protection of your personal accounts? * Only answer this question if the following conditions are met: Answer was 'No' at question '60 [**Q0060**]' (Do you feel that usernames and passwords are sufficient protection for your personal online accounts?)

Please choose all that apply:

- Multi-factor authentication (e.g. security tokens, smartcards with pins)
- One-time passwords Biometrics (e.g. fingerprint scanners)
- Certificate-based authentication (eg SSL client side authentication)
- Other:

Thank you for paricipating in this online survey. Please remember that all your question responses are kept confidential and no personally identifiable information has been collected. Please feel free to invite others to participate in this survey by sending them the following URL link: https://passwords.limequery.com/index.php/436563/lang-en

Appendix B

Character Groups and Password Cracking Times

Character Groups

Table B.1: Character Groups

Group	Characters in group	Total number of characters
Numbers	0123456789	10
Upper case letters	ABCDEFGHI-JKLMNOPQRSTUVWXYZ	26
Lower case letters	abcdefghijklmnopqrstuvwxyz	26
Special characters	!"#$%&'()*+,-.\/ :;<=>?@[]^_‘{|}∼	32
Letter (upper and lower case) and numbers	A-Z, a-z, 0–9	62
Letter (upper and lower case), number and special characters	A-Z, a-z, 0–9, !-∼	96

Password cracking times for character groups

These are the approximate crack times using brute force key search attack running on a modern personal computer (Halsey, 2012).

Key:

k – Thousand (1,000 or 10–3)

m – Million (1,000,000 or 10–6)

bn – Billion (1,000,000,000 or 10–9)

tn – Trillion (1,000,000,000,000 or 10–12)

qd – Quadrillion (1,000,000,000,000,000 or 10–15)

qt – Quintillion (1,000,000,000,000,000,000 or 10–18)

Table B.2: Password cracking times

Number of characters	Numbers only	Upper or lower case letters	Mixed upper and lower case letters	Letter (upper and lower case) and numbers	Letter (upper and lower case), number and special characters
4	instantly	instantly	instantly	instantly	instantly
8	instantly	13 mins	3 hours	10 days	57 days
15	46 days	212K years	28m years	97bn years	2tn years
18	126 years	3bn years	1tn years	23qd years	1qt years