THE FORGOTTEN PASSWORD: A SOLUTION TO SELECTING, SECURING AND REMEMBERING PASSWORDS

A thesis

submitted in fulfilment

of the requirements for the degree

of

Master of Social Sciences in Psychology

at

The University of Waikato

by

Tracy Jane Filmer-Clark

The University of Waikato

2008

Abstract

Internet passwords are required of us more and more. Personal experience and research shows us that it is difficult to create and remember unique passwords that meet security requirements. This study tested a unique method of password generation based on a selection of mnemonic aids aimed at increasing the usability, security and memorability of passwords. Fifty-one engineers, accountants and university students aged between 17 – 61 years participated in the study. They were randomly assigned to one of three groups: mnemonic, self-selection and random. All passwords in the study had to meet the following criteria: they had to be unique, at least eight characters long with a mixture of letters and numbers, and not include complete words or personal identifiers, sequential or repetitive numbers, and the passwords could not be written down or recorded anywhere. The mnemonic group created passwords based on a variety of mnemonic processes, the self-selection group generated passwords that complied with the above criteria, and the random group were assigned random passwords generated by the experimenter. Password recall was tested online once a week for three weeks, and then the passwords were renewed, with participants staying within the same groups for the length of the study. The second password was tested weekly for three weeks, then the passwords were renewed for the third and final time and tested for a further three weeks. The expectation was that the use of mnemonics in password creation would improve accurate recall of passwords, more so than if the password was 'self-selected' or a random password was assigned. The results showed that participants in the mnemonic group were able to accurately recall all three passwords significantly more often than participants in the self-selection and random groups. Furthermore, passwords created by the mnemonic group were more secure than passwords created by the self-selection group, as their passwords generated had a greater number of characters in them, slightly larger alphabet size, and a higher degree of entropy. The results are discussed in terms of the practical relevance of the findings.

Acknowledgements

I would like to thank my supervisors Drs Samuel Charlton and Nicola Starkey for their help and guidance in what, I had been lead to believe, could be a stressful experience and yet it was stimulating, challenging, and actually enjoyable. I acknowledge Sam as the instigator of this project, it was as a result of a practical applications project we had to complete in his level 3 paper Applied Cognitive Psychology. My thanks to Andrew for writing the program, and a big thanks to Rob for putting up with me frequently hassling him for data. Lastly, I would like to thank my family for their support throughout the whole process.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

1. Introduction

1.1 General

"It is a truth universally acknowledged, that…" (Austin, 1813, p.15) it is difficult to create unique, secure, passwords that can be accurately recalled at some later date. The difficulty lies not only in creating an original password, but that passwords are required of users in more and more situations. Research and personal experience shows us that it is difficult for users to create and remember a password that meets security requirements (Brown, Bracken, Zoccoli, & Douglas, 2004; Groves, 2002; Horowitz, 2001; Leonhard, 2006; Yan, Blackwell, Anderson, & Grant, 2004; Yap, 2001). Requirements such as; using a unique password, including at least eight characters with a mixture of letters and numbers, not using complete words or personal identifiers, sequential or repetitive numbers, and the most common security mistake – not recording the password anywhere.

Failure to meet security requirements can be costly. Using the same password for different applications makes all accounts vulnerable if at one site the password is breached (Gaw & Felten, 2006). Poor password selection, particularly using complete words exposes the password to dictionary attacks. Not only is poor password selection costly, but forgetting selected passwords can also be expensive and time-consuming for businesses. Research shows that forgotten passwords account for the highest instance of helpdesk calls, approximately 30 - 50%, and finance companies admit that it is even higher for them – a staggering 90% (Groves, 2002). To counteract this lack of security, many organisations force users to renew their passwords on a regular basis. This in itself leads to a form of rebellion, whereby the user resorts to even more insecure practices, such as writing all their passwords down.

In order to gain a better understanding of where we stand today with password use, effectiveness and inadequacies we firstly need to look at the issues surrounding password security, and the characteristics necessary for generating a secure password. Secondly, we need to examine password use, looking at the way users apply passwords, and the types of passwords chosen. The subsequent

sections will describe whether users can remember their passwords or not, and solutions for password memorability that have been offered and in some cases applied by researchers and practitioners. Finally, we will look further into the area of mnemonic aids; assessing cognitive principles that may apply to the area of password creation, use and memorability.

1.2 Password Security

As we move into a society whose core interactions are based on the transference of information via online technology, control over who has access to that information becomes vitally important. This section addresses the types and ways that passwords can be attacked. This is important, as the password is one of the first lines of defence. The use of passwords to ensure information security is likely to remain for the foreseeable future, for a range of practical reasons (Henry, 2007). Passwords work with nearly all combinations of existing software, hardware, and network systems. It is a fairly easy structure to implement, and creates a shared secret between the system and user, that can be accessed remotely. If combined with other methods of authentication, it can provide multiple layers of defence.

There are three main forms of password attack, they are: social engineering, technical subterfuge, and guessing attacks. Social engineering, as Granger (2001) puts it, "is a hacker's clever manipulation of the natural human tendency to trust" with the aim of obtaining access to valued information. This can be otherwise known as phishing, a term for 'password harvesting'. Whereby hackers masquerade as a trustworthy person. It is most often done via, email, the web, and instant messaging. Social engineering may also take the form of 'dumpster diving' – going through rubbish bins, or by 'shoulder surfing' – looking over people's shoulders as they enter their password (Henry, 2007).

Technical subterfuge covers many forms of attack but they are all a means of compromising host security. Henry (2007) provides a list of technical attacks. They include, passing-the-hash, rootkits, pharming, packet sniffing, keylogging, screenscaping, wiretapping, login spoofing, timing attacks, and identity

management system attacks. Henry (2007) goes on to note that no authentication mechanism (such as passwords) is safe against these two types of attack. They can, to some degree, be addressed by education in the first instance and greater technological protection in the second instance.

However, the main type of attack that applies to this study is the following type, guessing attacks. Guessing attacks consist of educated guesses, dictionary attacks, brute force guessing, and pre-computing. For pre-computing, crackers work out all possible password permutations, which are indexed to lookup tables, then all that is needed is just simple comparison with the password. Dictionary attacks are carried out in real time and use different dictionary files to crack passwords. They can be complimented by permutation of words, slang words, and numbers, that is, for each word, permute with 0, 1, 2 and 3 digits to construct possible password candidates (Yan, Blackwell, Anderson & Grant 2004). Passwords containing complete words can be cracked within seconds (Campbell, Kleeman & Ma, 2007). Brute force attacks are similar, in that they are in real time, except they try all combinations of all characters, and are only really feasible with short passwords (Henry, 2007).

Understanding these forms of attack, particularly guessing attacks, is the first step in developing a method of password creation that makes the password less vulnerable. The second step is to, in real terms, define the characteristics of what a secure password should consist of.

1.3 Recipe for a Strong Password

The recipe for a strong password consists of three characteristics/ingredients: alphabet size, character length, and entropy – which is affected by alphabet size and password length.

Alphabet size

A password can consist of letters, numbers, and special characters such as symbols and punctuation, or numerical codes which stand for characters (ASCII). The following are the number of items within each search space (alphabet size).

- 26 = alphabet (lower case)
- 36 = alphabet & digits
- 52 = mixed case letters
- 68 = letters, digits, symbols & punctuation
- 94 = keyboard enabled ASCII character set. Which stands for American Standard code for Information Interchange. Where the ASCII code is the numerical representation of a character

Character length

Character length is the number of items in a password. Table 1 shows the effect of search space (alphabet size) and character length on cracking time. As character length (and alphabet size) increases there is an exponential increase in cracking time and therefore an increase in security.

Table 1.

The effect of search space on cracking time

Alphabet Size / Password Length	26	36	52	68	94
3	.18s	.47s	1.41s	3.14s	8.3s
4	4.6s	16.8s	73.2s	214s	780s
5	112s	606s	3,820s	3,740s	73,400s
6	3,090s	21,800s	13.7 d	2.24 mo	2.63 mo
7	22.3 h	9.07 d	3.91 mo	2.13 y	20.6y
8	24.2 d	10.7 mo	17.0 y	145 y	1,930y
9	1.72 y	32.2 y	882 y	9,860y	182,000y
10	44.8 y	1,160 y	45,800 y	670,000 y	17,079,000 y
11	11.6 c	41,700 y	2,384,000 y	45,582,000y	1,605,461,000y
12	30,300y	1,503,000y	123,946,000y	3,099,562,000y	150,913,342,000y

(Source, GoedSoft, 2005, as cited in Henry, 2007)

Entropy

Entropy is a measure of disorder or randomness of the sequence of characters. As the alphabet size and character length of a password increases so does the entropy (as long as it does not contain complete words). “Entropy is a direct measure of password strength” (Henry, 2007, p.41). So, if a password has a large search space, that is, potentially contains letters, numbers, special characters and upper and lower case, as well as good character length (many sites suggest at least 8 characters, Yan, 2001), and a high degree of entropy, the password should theoretically be very secure/strong.

As the recipe for a strong password has become known, many organisations are beginning to enforce these rules by employing *proactive password checkers* within systems. Proactive password checkers test whether the password meets security requirements such as, no names, no words or reversed words, does not follow a keyboard pattern or only contain numbers, or is too short etc, (Klein, 1990). However, as Yan (2001) points out, they are expensive to implement and are unable to be applied to all systems. They are also complex and

error prone, take up a lot of space and take time to search (test the password). Proactive password checkers should also provide good feedback to the user if the password fails the check – which many systems do not.

The ingredients for a good password have been disclosed, but users do not follow the above advice, or many simply do not know what a secure password is, or the attacks it may be vulnerable to. The following section addresses this issue, looking at how users actually behave.

1.4 User Behaviour

Passwords are viewed by most people as a hassle, or as Groves (2002) puts it, 'a time-consuming hindrance' which inhibits users accessing information or sites quickly and easily. In conjunction with this negative attitude towards the use of passwords, as mentioned previously, users tend to have little or no education about the security issues surrounding password use. Even if they are educated, people as a whole tend to take shortcuts, unless they are personally motivated to maintain secure practices, or if the system is usable (Weirich & Sasse, 2002). User password habits can be broken down into three categories: types of passwords chosen, the way those passwords are used, and whether they can remember them or not. Statistics available from current literature on the way passwords are used is addressed in the next section, followed by the types of passwords chosen, and then later we deal with the memorability of passwords.

1.4.1 Password Use

SafeNet (2005) showed in their 2004 global password survey that 50 percent of employees write their passwords down. Sixty-seven percent of people have five or more applications that require passwords, and a further 31 percent access nine or more applications. Eighty percent of participants use the same password for multiple applications, and 47 percent require passwords to be reset at least once a year. These findings are similar to those reported by Brown, Bracken, Zoccoli and Douglas (2004) in a survey of 218 undergraduate students 54 percent indicated that they kept a written record of passwords. On average,

students had 8 password applications, and used approximately 4.45 different passwords to cover those sites.

The SafeNet (2005) survey also revealed that at least one third of respondents shared their passwords with other people. Weirich and Sasse (2002) confirmed that many people in organisations succumb to the social pressure of disclosing passwords to colleagues in times of need; as it otherwise implies a lack of trust. Leyden (2003) also reported that 75 percent of employees know their co-workers passwords.

1.4.2 Choice of password.

One practice is primarily using names and birthdays for constructing passwords. Harada and Kuroki (1996) found that 42 percent of people surveyed reported using their own names as passwords. Brown, Bracken, Zoccoli and Douglas (2004) found over 90 percent of participants in their study used the 'self' as a basis of password construction. Or, as Leyden (2003) found, 12 percent of people used the word 'password' as their password. British psychologist, Helen Petrie (as reported by Andrews, 2002) stated that password choice could be inadvertently revealing, as they are usually chosen on the spot, with whatever readily comes to mind. She identified four password genres while analysing the responses of 1200 participants in a British survey. Firstly, "family-oriented" passwords, which are passwords that either include the person's name, the name of a close family member, pet or a birth date. Secondly, passwords based on "fans", using the name of singers, movie stars, athletes, fictional characters or sports teams. "Fantasists" was what she named the third category, with an interest in sex evident in the choice of passwords. The last group, with approximately 10 percent of the respondents, she called "cryptics"; people who used passwords consisting of random strings of letters, symbols or numbers.

1.5 Studies of Password Memorability

Recalling passwords is not a simple case of having a go until you can remember it. Many systems only allow three attempts at entering a correct password and then restrict access. Most people then seek helpdesk assistance, or

click ‘forgot password’ and have their password reset electronically. This exercise can cause frustration for users, and can be a time consuming, and costly exercise for Information Technology (IT) departments.

Dhamija and Perrig (2000, as cited in Brown, Bracken, Zoccoli & Douglas, 2004) found an accurate recall rate of 70 percent for passwords created a week previously by participants. They were passwords that had not been used before which they (the participants) considered to be secure.

Leonhard (2006) tested the memorability of three types of random password generation algorithms. The first was an AlphaNum algorithm, which created a random password six characters long using upper and lower case letters and numbers, with a total of 62 possibilities per character. The second system was a Diceware Generator algorithm producing random lists of words, such as; ‘doze stuff salve’, ‘ample acidic leery’. The third was a Pronounce3 Generator which generated passwords that were pronounceable in English, using syllables based on their frequency in English writing, for example: abdaumso, cudawigo, urcezfae. Leonhard found little difference between the types of algorithms and only a total of four people out of 19 remembered their passwords after a two-week delay.

The study by Brown, Bracken, Zoccoli, and Douglas (2004) also found that out of 218 students, 31 percent had forgotten passwords and 22 percent had experienced password mix-ups. The researchers found that the cognitive aspects of password creation, use, and recall had received little attention in the psychological literature. Yan, Blackwell, Anderson and Grant (2004) also highlighted the need for intervention at the password generation and renewal stage, when clear instructions about creating and memorizing a strong password should be given to users.

Since there exists a tension between the need for security, with the need for usability and memorability, researchers have been testing various password systems to find a balance between them. Jeyaraman and Topkara (2005) looked at a way of generating mnemonic based passwords. Mnemonics are memory tools, and in this instance they refer to generating a password phrase or sentence to aid with password recall. The researchers proposed using the headlines from news stories to form passwords, as headlines tend to be simple, concise and memorable.

From the headlines, semantic variants of each word would then be created, for example, if the heading had the word ‘plane’, it could be changed to airplane, drone, glider, or helicopter, and the sentence would still make sense, but not exactly match the original. The sentences can then be encoded mnemonically by either using the first letter of each word, or the last letter of each word to form the password, or the n^{th} letter of each word. Numbers could then be embedded into the password by, for example, changing ‘o’ to ‘0’. Upper-case letters could be incorporated by placing capitals where they would normally occur in natural language text, such as a capital for the beginning of the sentence or for names and places. At this stage, this method of password generation has not been tested, so it is not known how effective or usable it is in practice.

Another method that has been created but not yet tested is a system by Topkara, Atallah, and Topkara (2007), it takes the previous system one step further. A mnemonic password is generated by word substitutions of a news headline. It is then applied to a ‘helper card’, which is a grid with the website application written on the side, such as ‘Amazon’ and next to it is the beginnings of the password, for example, ‘T-%7’ the mnemonic is then used on the grid (which has the alphabet across the top) to complete the password. For example, ‘b’ stands for ‘!’. The password generated is very strong, yet the method is fairly convoluted, and the ‘helper card’ must be kept in a secure, yet accessible place, and must be regenerated whenever passwords are renewed.

Lu and Twidale (2003) took a different approach to managing multiple passwords. Their system was based on the premise that if a few ‘hints’ were given about the password, it would jog users memory. The system was called Minimal Feedback Authentication (MiFA). Users could decide which parts of the password they would be happy to reveal, a snapshot image of the login and password would then be taken and the chosen characters semi-revealed and the rest represented as ∗. An example given by the researchers can be seen in Figure 1. The image could then be stored on a local machine, along with other passwords for other sites. However if they were logging on using a different machine, they would then have to recall the password without the help of the image. Results from a pilot study

(five participants) were fairly promising with 66 percent of passwords created using MiFA correctly recalled 10 days after they were created.

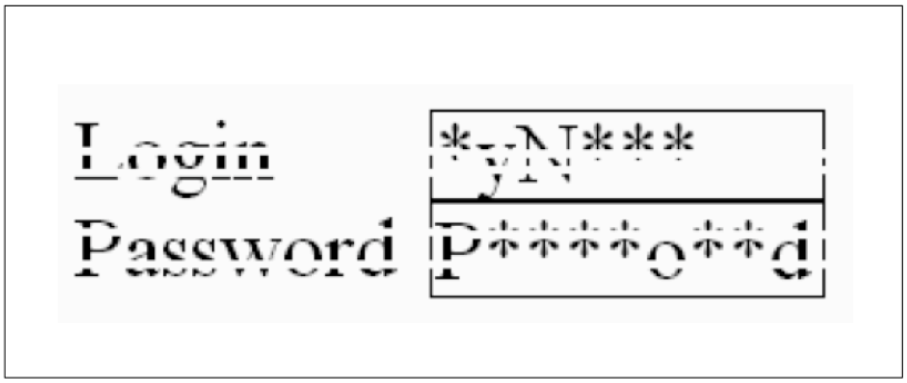


Figure 1. A MiFA snapshot image of the login "MyName" and password "Password" (Source, Lu & Twidale, 2003). Note: image is deliberately degraded to thwart password-cracking software.

A comprehensive study carried out by Henry (2007) focused on password strength. The assumption was that passwords over 20 characters long would be very strong. His study used 139 participants, familiar with information technology, who were divided into four groups. The participants were allowed to choose one of five methods for creating their passwords. These were: *The Old Address,* which involves spelling out an old, but unforgettable address. *Unexpected Nonsense,* Ferguson and Schneirer (2003, as cited in Henry, 2007) recommended the use of unexpectedly nonsensical passphrases as passwords. Their example was, "Pink curtains meander across the ocean". *The Acrostic,* which draws the first letter out of a phrase, instead of the complete word, as in the previous two methods. *The Old Memory,* (Burnett 2006, as cited in Henry, 2007) uses questions such as, "What was your favourite place to visit as a child?" The answer to the question was the password. *The Confession,* is a password that is a confession of something personal that the participant does, such as "I pick my nose and eat it". The final choice available to participants was to use their own method of password creation.

Once passwords had been created, participants were allowed to print out or write down the password, as a backup. They were then required to login and enter their password online once a week, for seven weeks. All participants in the four groups were allowed to choose which password system they used. Manipulated by the experimenter were the number of examples of password given (for the type of password method chosen), and the number of times participants were required to re-enter their passwords after generating them. The results showed that failure to recall passwords for the different types of passwords used ranged from 68 and 65 percent, for the Address and Acrostic groups respectively to 31 percent recall failure for the Nonsense group. With the number of attempts at password recall over the seven weeks ranging from 32 attempts for the Nonsense group to 109 attempts for the confession group.

As stated by Henry (2007), the overall results showed that "30 percent of participants generated and used very strong passwords without failure for seven weeks", (p.8). This appears to be a high proportion of failure, especially when participants had access to the correct password. The number of times that the password was re-entered at the generation stage, and the number of example passwords given had no effect on accurate recall. Henry surmises that the reasons for password failure are complex, and some users may require additional attention and resources to help resolve problems.

All told, there has not yet been a resolution between the need for security with the desire for memorability and usability regarding passwords. There is the practical issue of needing 100 percent memorability, an errorless performance, for the password system to work. This leads to the next section, the use of mnemonic aids for improving the creation, use and memorability of passwords.

1.6 Mnemonic Aids for Passwords

The use of mnemonic aids to assist with recall of information has been around for a long time. The Method of Loci (place) is possibly the oldest known mnemonic device, and was used by the Greeks in 500 B.C. It is the process of visualising a well-known room or place, and then placing items that need to be remembered within that room (Lea, 1975). Retrieval of the items can be carried

out by mentally walking through the room. Miller, Galanter and Pribram (1960) described the Pegword method of associating rhyming words with numbers, for example: '1 is a bun', '2 is a shoe', '3 is tree'… items to be remembered could then be 'hooked' onto the rhyme. This method was particularly useful when trying to remember numbered or ordered information. Paivio (1965) proposed that concrete words could be visualized (and therefore recalled) better than abstract words, which cannot be visualized. His hypothesis was supported, imagery assisted with the ease and accuracy of recall. However, these mnemonic aids, particularly the first two, are not on the whole appropriate for passwords, there are other mnemonic aids that may help with encoding and retrieval of information, that may be more pertinent to passwords.

One such aid recommended is the Meaningfulness Effect, demonstrated by Underwood (1964), whereby the number of letter pairs recalled by participants was superior when the letter pairs were meaningful. Another aid to retrieval is the level of processing carried out at the time of encoding. Craik and Lockhart (1972) proposed that incoming information could be processed at different levels, from shallow to deep and that the particular level of processing implemented affected the durability of memory, the processing was otherwise known as encoding. Structural encoding emphasized the physical structure of the stimulus and is fairly shallow processing. For example asking whether the word to be recalled is in upper or lower case is a form of shallow processing. Intermediate processing is phonemic encoding which looks at what a word sounds like. Semantic encoding addresses the actions and objects the word represents; it is a deep level of processing which produces more lasting memory. Yet Rogers, Kuiper and Kirker (1977) showed that information relating to 'self' – known as self-referent encoding – demonstrated even superior recall than semantic encoding. Anderson (1976) showed that elaboration had an effect on memory, that is, if the material to be encoded is elaborated on, and that elaboration is a product of the person's real-world experiences then encoding is enriched and recall improves. All four of these findings (meaningfulness effect, depth of processing, self-referent encoding, and elaboration) suggest that enriching the encoding process in various ways increases the memorability of stimuli in ways that could be useful in the context of password applications.

The Generation Effect (Slamecka & Graf, 1978) presented another aid to retrieval. The researchers found that recall performance was superior for words generated (chosen) by the participants, compared to words simply presented to participants to remember. Another aid is using a cue (which is a hint or starting point) at time of recall, as the use of a cue has been found to help with retrieval of originally encoded information (Beal, 1985). If there is prior knowledge of the subject encoded then, information can be stored in chunks rather than individual items (Gobet, Lane, Croker, Cheng, Jones, Oliver, & Pine, 2001). Taken together with the previous methods of enriched encoding, self-generation, retrieval cues, and chunking provide additional mnemonic aids to improve memory recall. To gain a greater understanding of encoding and retrieval, looking at what hinders recall and common errors made at the retrieval stage may also help in the password selection process.

Forgetting can be due to decay and interference. Decay theory proposes that the link – memory trace – between a cue and target memory decays over time, but rehearsal of the memory will refresh the trace (Thorndike, 1911). However, as McGeogh (1932, as cited in Nairne, 2002) stated, some memories fail to decline over time, and may even improve with time. He proposed that it is what occurs over the process of time such as, interference, that affects recall. Two types of interference that may occur are retroactive and proactive interference. Retroactive interference occurs when current learning interferes with earlier learning. While proactive interference occurs when old information interferes with new information. An example of this, regarding the present study, would be an old password interfering with the recall of a current password. There can be a release from proactive interference if the stimulus material is changed (Goggin & Wickens, 1971), such as changing the category of a password. Confusion at the retrieval stage may also occur if there is more than one memory associated with a single retrieval cue, this is known as cue overload (Watkins & Watkins, 1975).

Specifically looking at the memorability of passwords, Vu, Proctor, Bhargav-Spantzel, Tai, Cook, and Schultz (2007), analysed the types of recall errors that users made when using a sentence generation mnemonic technique for password creation. The most common error was a *sentence* error – participants forgot the sentence or the exact wording of the sentence. The second most

frequent error was *special character/digit* error, which occurred when the special character or digits used were forgotten. Thirdly *association* errors occurred when participants used the password from a different account. Next *sentence and special character/digit* errors occurred when participants forgot the sentence generated and/or the special character or digit. Finally, *order* errors occurred when the contents of the password were recalled but the sequence was forgotten. There may be other types of errors that occur for different password generation systems.

The sentence generation technique used by Vu et. al. (2007) had participants make up a sentence with at least six words, taking the first letter of each word to form the password, with some participants required to embed a special character and/or a number into the password. The passwords created were strong, but at the cost of memorability. This result was also found by Henry (2007) and reiterated by Sasse, Brostoff and Weirich (2001) who reported that "both security and usability experts have stated that recalling strong passwords is a humanly impossible task because strong passwords are non-meaningful items and hence inherently difficult to remember" (p. 126). In those instances, it may be so, however the sentence generation technique is only one mnemonic tool, which may involve self-generation, but does not include self-referent encoding, elaboration, chunking and the use of cues to improve recall performance. A method of password selection that incorporates a variety of mnemonic tools may be the solution to the 'forgotten password'.

1.7 The Present Study

An overview of current literature regarding password selection, use and memorability shows that firstly, many people do not understand what a secure password is and why it is necessary to implement secure password practices. Secondly users have difficulty creating passwords that can be recalled at some later date, and therefore resort to writing passwords down or using the same password for multiple accounts. Research in this area has begun to look at ways of addressing these problems, namely applying mnemonics to the password process. However, mnemonic passwords have been investigated in only a few studies, and

performance was not as good as it needs to be for practical use, that is 100 percent accurate recall to allow access to required sites or information. Yet, encoding effects in memory literature suggest some additional procedures show promise for password applications. The purpose of the present study was to investigate whether a procedure to aid participants in generating meaningful, self-referential, and elaborated passwords, incorporating the use of a cue, would be of practical use.

We anticipated that passwords produced by means of mnemonic process would have higher accurate recall rates than randomly generated passwords or passwords selected by participants without the mnemonic process. Secondly, we expected that passwords produced via the mnemonic process would be recalled with high levels of accuracy over distributed recall periods, more so than if the passwords were 'self-selected' by participants or if they were randomly assigned to participants. Thirdly, we predicted that passwords produced utilising mnemonic aids would be subject to less interference (namely proactive interference) when passwords are changed, as compared to the other two methods of password generation (self-selection and random). Finally, we anticipated that passwords produced by the use of mnemonic processes would be more resistant to password attacks, that is, have a greater degree of entropy than self-selection and randomly assigned passwords.

A further aim of this study was to ascertain password user habits and collect general demographic information about participants. In addition to testing the working memory capacity of participants by administering the WAIS-III, digit span sub-test, for the reason that working memory capacity may influence participant's ability to receive, store and retrieve information.

2. Method

2.1 Participants

Thirty-three professionals from a number of organisations within the Waikato, the majority of whom were employed in the Engineering and Accountancy professions, participated in the study, along with 19 first year psychology students from Waikato University. A total of 52 participants were recruited, with one participant withdrawing after three weeks due to personal reasons. The mean age of the participants was 32.46 (SD = 11.77), and the range was from 17 to 61 years. The participants included 19 males and 33 females. Working memory scores for participants ranged from 3 – 14 (14 being the highest possible score).

Participants from the workforce were recruited by approaching engineering and accountancy employers in the local area. These professions were chosen because of their frequent use of passwords. A brief description of the study and the requirements for participation were explained. Once consent was obtained from management, employees were then approached, and given written and verbal instructions on what the study entailed (see instruction sheet in Appendix A). If the employees were happy to proceed, they then completed an informed consent form (see Appendix B). Two prizes with a combined value of $300 were drawn by an independent party at the conclusion of the study and allocated to two of these participants.

First year psychology students were recruited by placing a flyer on their online message board, a copy of the flyer can be seen in Appendix C. An appointment was made to meet with those showing interest in the study to further explain what participation entailed. Informed consent was obtained from those wishing to participate. Two course credits were assigned to students who participated in the study.

Data collated from the background questionnaire revealed that participants had on average 6.3 applications that required passwords and of those applications, 3.9 of the passwords were unique. That is, many reused the same password for

more than one application. There was no significant correlation found between the number of passwords participants had and correct recall of passwords; that is, there was no evidence that the more passwords a person had to remember, the more difficult it was to accurately recall the passwords.

Seventy-nine percent of participants had forgotten a password, and had contacted a 'help desk' to have the password reset. The main type of passwords created by participants was a mixture of complete words (including names) and numbers. Eighty-eight percent of participants were asked (on average, at two sites) to renew their password at various intervals, mostly every 60 days.

2.2 Materials

Three instruments were used as experimental materials:

i. A background questionnaire
ii. Working memory test (Backward Digit Span)
iii. Retrospective post-study questionnaire

The background questionnaire consisted of 10 questions asking about participant's current password habits. Questions one to five asked; how many passwords were required of them, how many unique passwords did they have, how often were they asked to renew them, how often did they actually renew them, and did they write them down? Questions six and seven enquired about whether they had ever forgotten a password or contacted a 'help desk' to reset a password. Participants were then asked to indicate which type of password they most often used, out of a list of possible methods; for example, names, words and numbers. Demographic information, such as age and gender, was also requested (see Appendix D for background questionnaire).

The digit span, verbal subtest of the Wechsler Adult Intelligence Scale, version three (WAIS-III) was administered. A list of two to nine digits was read aloud, the participant repeated back the digits. This was then repeated, but the participant repeated the digits back in reverse order. Backward Digit Span (BDS), in particular was assessed as a measure of working memory capacity. A deficit in working memory function may contribute to an anomaly in the results.

The retrospective post-study questionnaire was sent to participants as a hyperlink with their final password recall request (3rd recall of 3rd password). The retrospective post-study questionnaire consisted of eight questions. The purpose of the questionnaire was to find out how easy or hard the passwords were to create and recall. The questionnaire asked what, if any, systems did the participant employ to remember the password, and did any of the previous passwords interfere with remembering the current password? The participants were also asked to recall, if possible, all three passwords used in the present study (see Appendix E for post-study questionnaire).

2.3 Procedure

The study was a mixed design with three levels of the *between-group* factor, password type, and three levels of the *within-group* factor, password renewal. Figure 2 shows a visual representation of the process involved. The independent variable of *password type* was manipulated by randomly and evenly assigning participants to one of three groups:

i. **Mnemonic**, passwords, created according to proven cognitive principles for encoding, memory and recall.
ii. **Self-selected**, passwords chosen by participants.
iii. **Random** passwords created by the experimenter and assigned to participants.

The second independent variable, *password renewal*, was manipulated by requiring each participant to recall three successive passwords. In addition, each password was tested for recall three times, a week apart. This provided a dependant variable, *correct/incorrect*. Participants were allowed up to three attempts at entering a correct password, which generated another dependant variable – *number of attempts per trial*.

All three groups had the same criteria for creating passwords, as outlined in Table 2. The criteria were adopted from the standards set for passwords by most banks, and in this instance, the Westpac Bank. The *self-selection group* were asked to create a password based on the criteria in Table 2 (the instruction sheet

for the self-selected group can be seen in Appendix F). Participants in the *random group* were given a random password, generated by an online random password generator that met the password criteria. An example of a random password given to participants in the random group can be seen in Appendix G.

The *mnemonic group* used a system of password creation based on proven cognitive principles for encoding, memory and recall. A summary of the mnemonic instruction sheet is shown in Table 3, and the complete form can be seen in Appendix H.

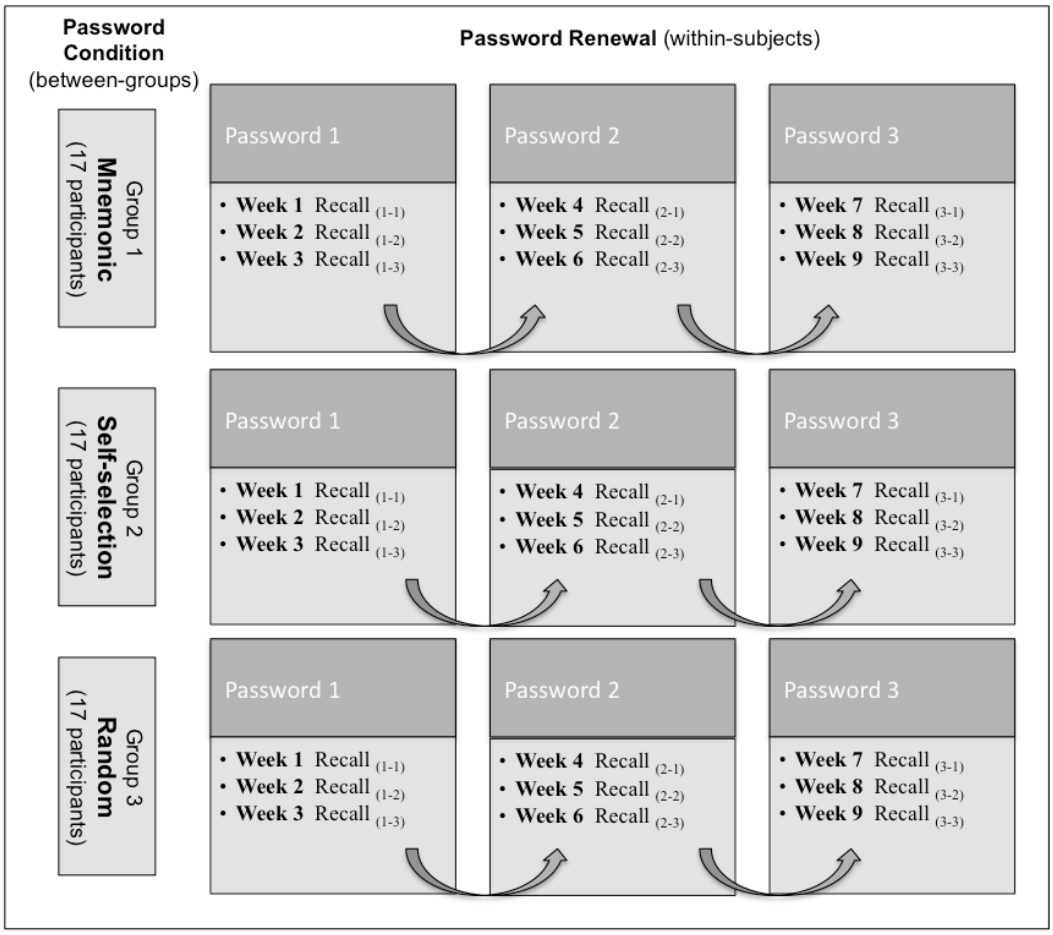


Figure 2. The mixed experimental design used in the present study.

Table 2
Criteria for all Passwords

8 – 12 characters long (at least 1 letter & 1 number, can include special characters). • Must be unique. • Not easily guessed, or relate to known personal information, such as, birthdays, names, words or telephone numbers. • Cannot use sequential or repetitive numbers such as, 4321 or 444 • Cannot contain complete words • In essence, the password must *appear random* • **Cannot share your password with anyone else.** • **Cannot write down or record your password.**

Table 3
Mnemonic Group Instructions

• Think of a category of something that interests you, for example, cars, a sport, music etc • Within the category think of three or four different items that fit into it. They can be more than one word and can also have a number in them. • List the items. If they do not include any numbers then add a number to the front or back of the item. Some examples are: Rugby — Music Bands Dan Carter 12 — 1. Foo Fighters Jo Rokocoko 14 — 2. Artic Monkeys & Richie McCaw 7 — 3. Led Zeppelin! • Underline the first letter of every word and every number. Then list the underlined letters and numbers to the side, as below. These letters and numbers are the password. • Write out the password, saying to yourself what each item is, as you write it. • Repeat these steps, if necessary, until the password has been learnt and can be repeated without looking at the paper. • Write down the category heading, e.g. Rugby to use later as a password **cue.** For example: Rugby — Music Bands **D**an **C**arter **12** **DC 12** — **1** **F**oo **F**ighters **1 FF** Jo **R**okocoko **14** **JR 14** — **2** **A**rtic **M**onkeys **&** **2 AM &** **R**ichie **M**cCaw **7** **RM 7** — **3** **L**ed **Z**eppelin**!** **3 LZ !** **= dc12jr14rm7** *Cue: Rugby* — **= 1ff2am&3lz!** *Cue: Bands*

Participants were seen individually either in an office at their workplace or at an office at the University. After consenting to participate, they completed the background questionnaire (see Appendix D). The digit span subtest of the WAIS-III was then administered to assess working memory function.

Participants were then randomly and evenly assigned to one of the three groups. The participants were then asked to create, or were assigned a password, based on the criteria set for each group. They were then directed to a computer where the password login webpage was displayed. They logged on using their email address, and then entered their password. An example of the login page can be seen in Figure 3. To thank them for their participation, a chocolate bar and drink was offered.

A week following the initial assignment of passwords, participants were sent an email (see Figure 4), with a hyperlink connecting them to the login page (Figure 3). They entered their user name – which was the email address that the participant was using for the study – followed by their password. The password characters typed were suppressed and instead shown as black dots, this along with allowing three attempts at entering a correct password, was implemented to create a login system that matched real-world login sites. Participants in the mnemonic group were also given their password *cue* when emailed (see Table 3). This was known as the first recall of the first password $R_{(1-1)}$, as seen in Figure 2.

Information entered on the login page was saved to a remote authentication server. The server recorded the attempts made, whether the password entered was correct or incorrect, and the number of attempts used. The login username and password had to be 100 percent accurate to receive a 'correct – thank you for participating'. The passwords were also case sensitive.

Two weeks after the initial password was created, participants were emailed again and asked to enter their password into the login page for the second time, $R_{(1-2)}$ – password one, second recall (see Figure 2). This was repeated again the following week ($R_{(1-3)}$). At this stage, participants were seen again, and asked to create or be assigned a new password – using the same instructions that they were initially given – this was known as *password renewal*. The second password was tested for recall a week later, $R_{(2-1)}$ and again, two and three weeks after

renewal ($R_{(2-2)}$ and $R_{(2-3)}$). After the third recall of the second password, the password was renewed for the third and final time and then recall was tested for the following three weeks ($R_{(3-1)}$ to $R_{(3-3)}$). Each time participants renewed their password, chocolates were offered as an appreciation of their involvement. A visual representation of the password process is shown in Figure 2.

Along with the final email for the 3rd recall of the 3rd password, an additional hyperlink was included. The hyperlink connected participants to the retrospective post-study questionnaire, which was completed online. Participants were also thanked for their involvement.

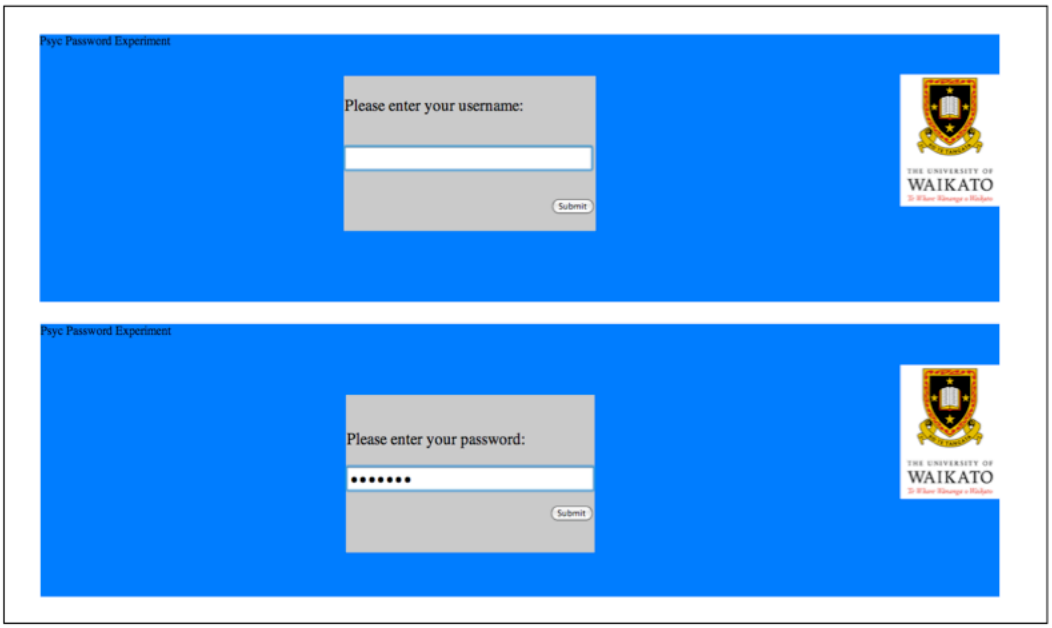


Figure 3. Password login screens for participants.

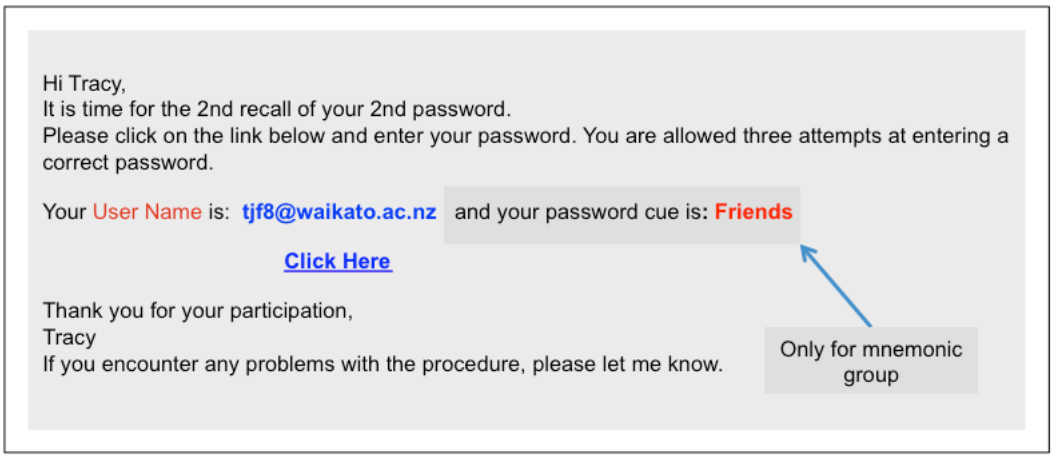


Figure 4. Password reminder email sent to participants.

3. Results

3.1 General

The following results are, for the most part, laid out in the order of the hypotheses made in the Introduction. The first section looks at accurate recall of passwords, comparing the results found for each group. In conjunction with accurate recall, the number of attempts made at each password trial is compared across groups. Also with respect to the accurate recall of passwords, the results from the retrospective post-study, asking participants to recall all three passwords, are portrayed. The second section considers and assesses the strength of the passwords that were created throughout the study. Finally, error analysis of incorrect password recall and the subjective findings for each group were looked into further.

3.2.1 Group differences – Accurate recall of passwords.

Figure 5 shows the mean percent correct recall for each group and the 95 percent confidence intervals. A one-way Analysis of Variance (ANOVA) was conducted using the percentage total correct recall per participant for all trials completed, between the three groups. The difference between groups was significant, $F(2,49) = 11.84$, $p < .001$. Levene's test for homogeneity of variances was significant ($p < .05$) showing that the sample variances for each group were not equal. This may have been due to the lack of variance within the mnemonic group. The percentage correct recall ranged from 62.5 – 100% in the mnemonic group, and the range was 0 – 100% in both the self-selection and random groups. The unusual variances across conditions could be attributed to the very high performance of the mnemonic group (SD = 13.20) relative to the self-selection (SD = 33.80) and random (SD = 33.78) groups. A Shapiro-Wilk test for normality showed that the distribution of the self-selection and random groups was within normal range. However, the distribution of the mnemonic group was not normal. Tukey's HSD post hoc test showed that the mnemonic group had a significantly different percentage correct recall than the self-selection and random groups, ($p < .001$). The test also revealed two homogeneous subsets, the self-selection and the random groups in one set, and the mnemonic group in the other.

Since the homogeneity of variances and normality assumptions of ANOVA were not met, recall accuracy of the three groups were then analysed separately using a Kruskal-Wallis Test. Figure 6 provides a visual representation of the percentage correct recall for each password across the three conditions. The test showed that the differences in correct password recall between groups, for all three passwords, were significant, χ^2 (2, n = 51) ≥ 6.50, p < .05.

The results were further broken down to compare correct recall per group for each password trial (nine trials in total, three passwords tested three weeks each), shown visually in Figure 7. To compare the correct/incorrect results for each password recall trial between each group, a Pearson Chi-Square test was conducted. All recall points showed a significant difference between groups, χ^2 (2, n=51) ≥ 7.95, p < .05, apart from recall $R_{(2-1)}$ and $R_{(2-2)}$, χ^2, (2, n=49) ≥ 3.09, p > .05. The exceptions can be seen visually in figure 7.

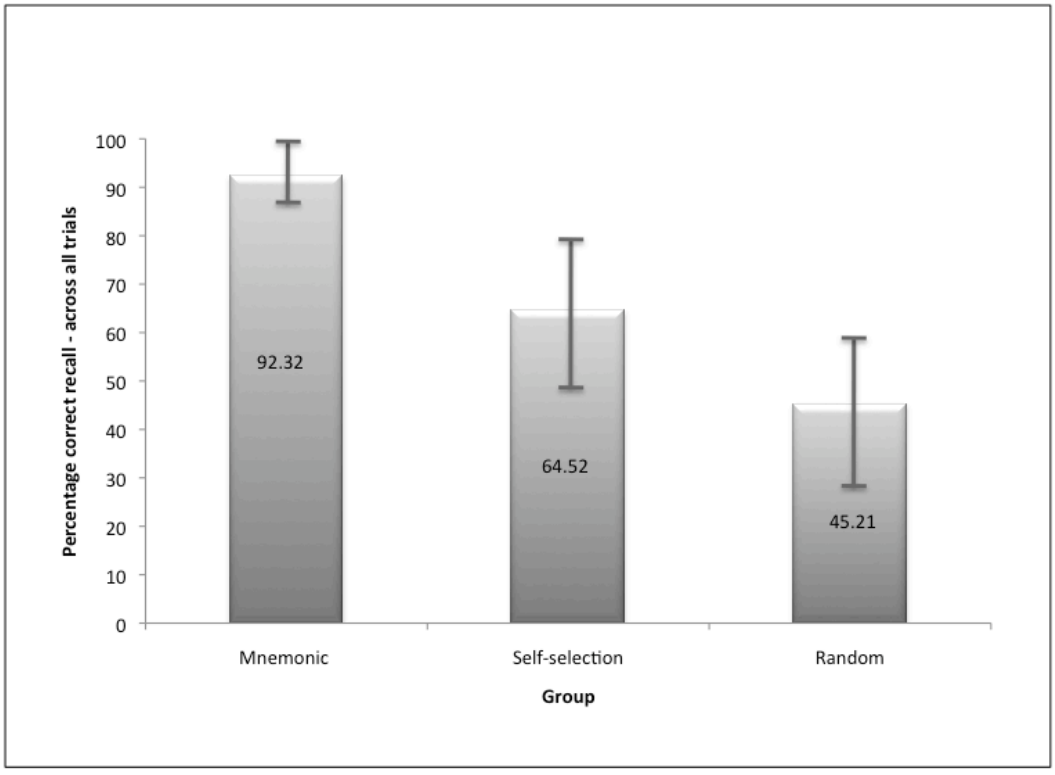


Figure 5. The mean percentage total correct recall across all trials. The shaded bars show the mean scores and the vertical bars represent the 95% confidence intervals.

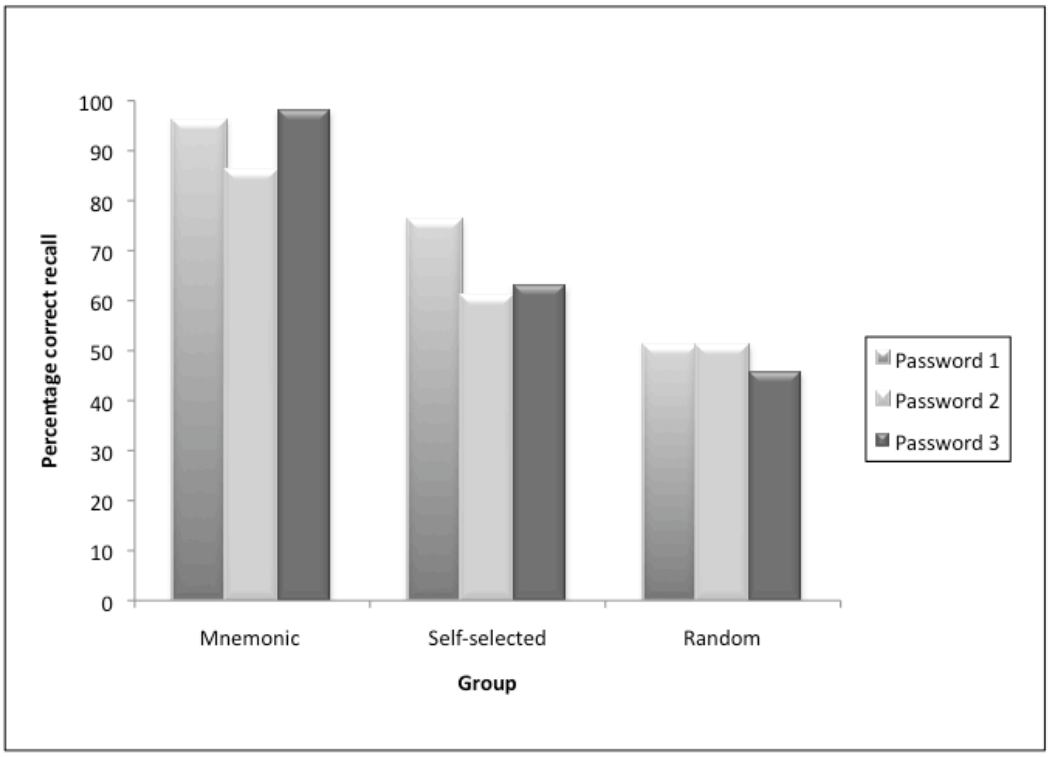


Figure 6. Percentage correct recall per password for each group.

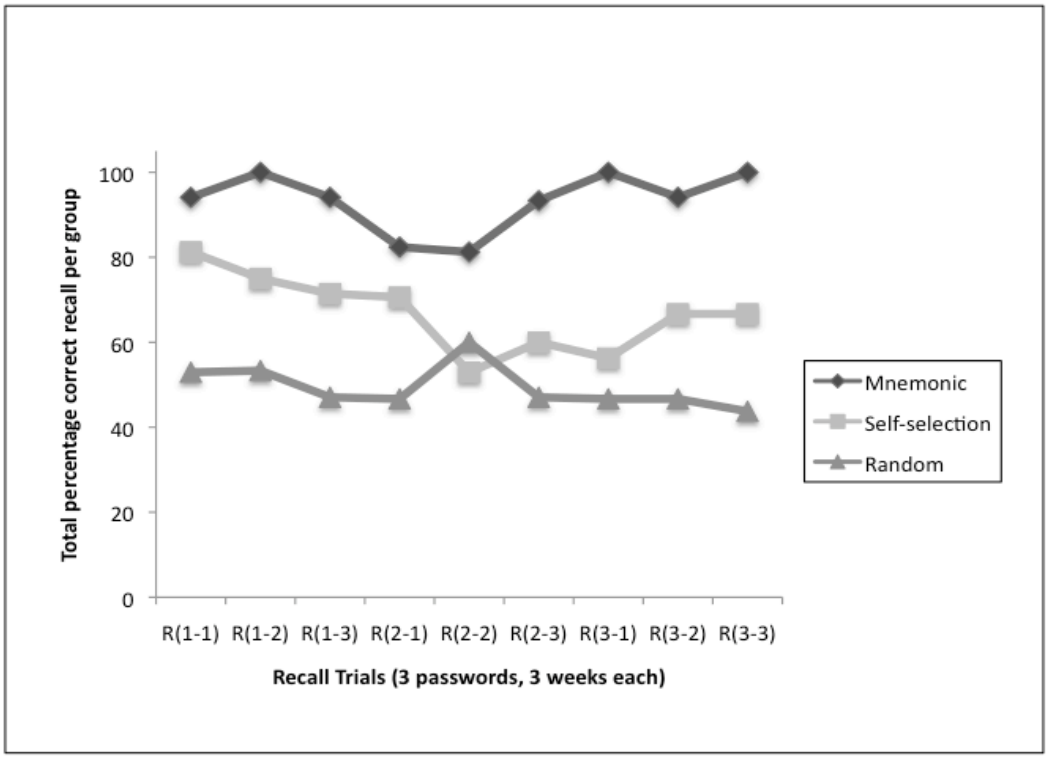


Figure 7. Correct recall of passwords for each group, shown across each trial.

3.2.2 Password attempts.

A further test of password accuracy was to calculate the number of attempts taken to gain a 'correct' trial or, on the other hand, how often all three attempts were used without achieving a correct answer. Figure 8 shows the average number of attempts used at each password recall trial, for each group. The mnemonic group had noticeably less attempts per trial than the self-selection and random groups. However, Figure 8 may be somewhat misleading as some participants mentioned that when they knew they were unable to remember their passwords they didn't even attempt a guess. To gauge how often this may have occurred the number of trials missed by participants, were summed for each group and can be seen in Figure 9. (This in itself, however, may not be conclusive as some participants were away on holiday during the study and were unable to attempt some trials). Taken together, the findings from Figures 5 - 8 illustrate that accurate recall of all three passwords was superior for the mnemonic group in comparison to the self-selection and random groups.

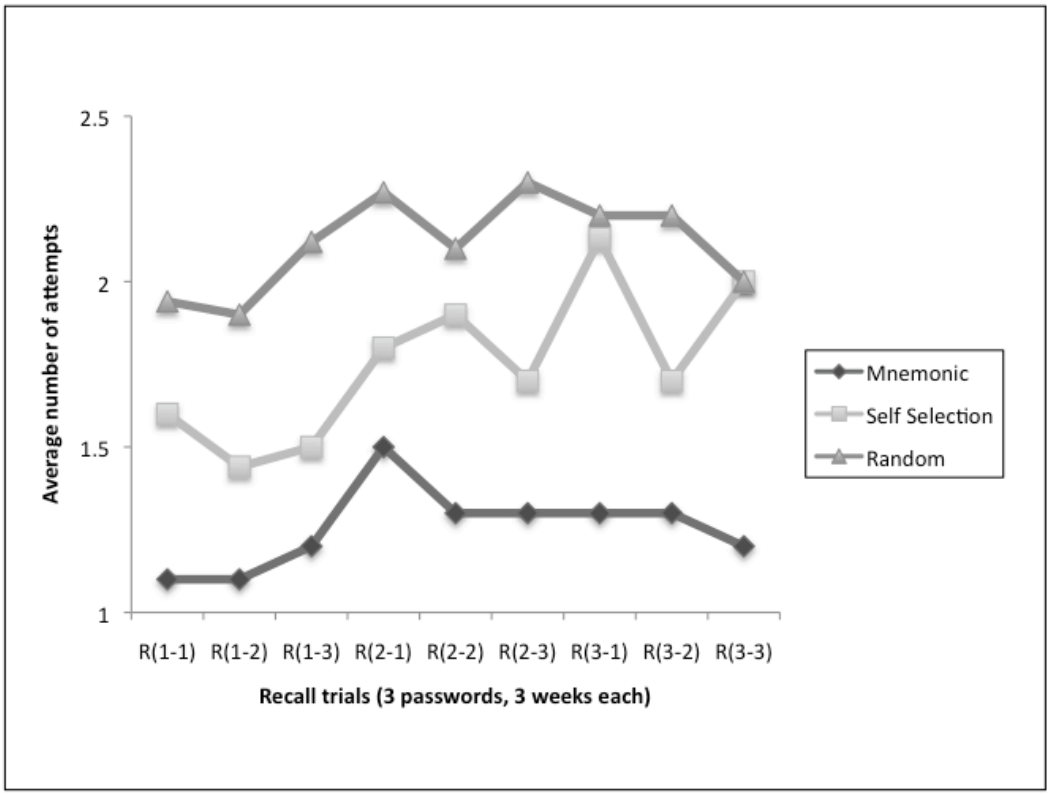


Figure 8. Average number of attempts made per password recall trial, with a maximum of three attempts allowed.

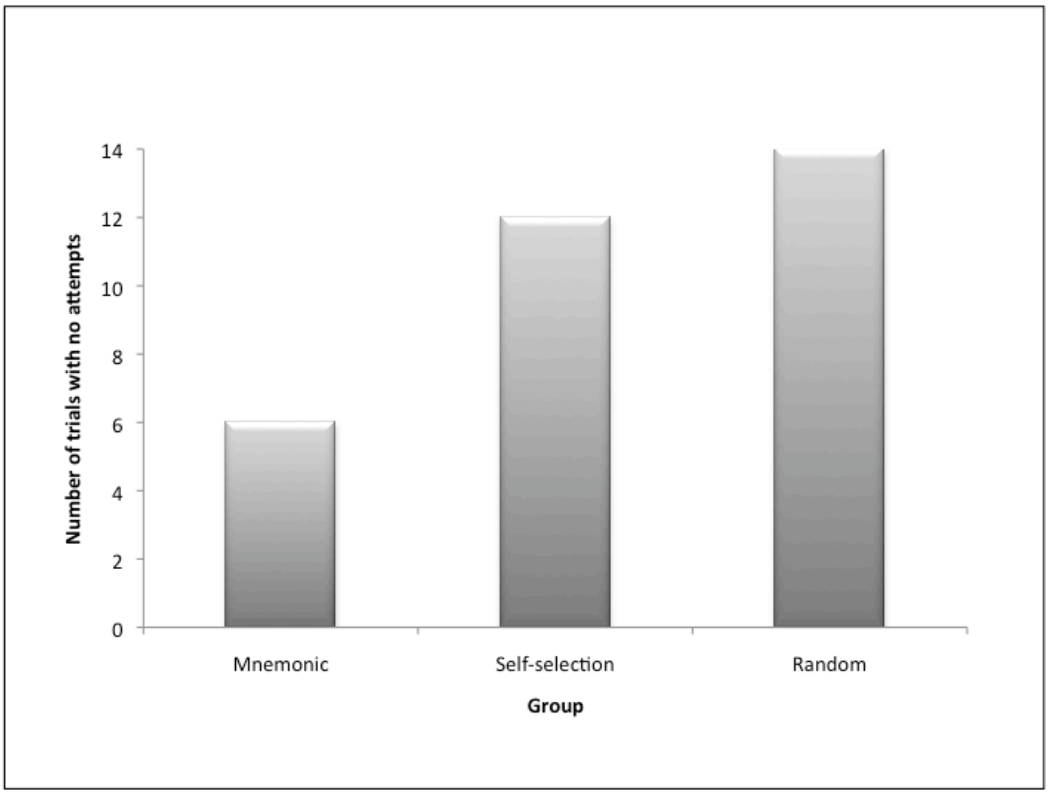


Figure 9, Total number of trials for which participants did not make any attempts at password recall.

3.2.3 Analysis of individual differences.

A Levene statistic for homogeneity of variances for both BDS and age of participants was not significant, so we can assume that the population variances for all groups are approximately equal. There was no correlation found between ages of participants and working memory score (BDS), $r = .48$, $p > .05$. There was also no significant difference in working memory scores, $F(2,48) = .54$, $p > .05$, or age of participants between the three groups, $F(2,49) = .82$, $p > .05$. No significant correlation was found between age of participants and the percentage correct total recall, ($r = -.04$, $p > .05$). In light of these findings, no analyses of covariance were conducted. However, there was a significant negative correlation between age of participants and the number of passwords that were required of them in every-day-life ($r = -.44$, $p < .01$), indicating that younger people in the present sample reported needing a greater number of passwords than the older participants.

3.3 Retrospective Post-Study Password Recall

At the completion of the study, participants were asked to complete an online questionnaire. As part of that post-study questionnaire, participants were asked to recall all three passwords (if possible). The overall response rate for completing the questionnaire was 76 percent of participants. Figure 10 shows the correct recall of all passwords after the conclusion of the study. A Chi-Squared test comparing the probability of correct recall of the three passwords across the three groups was conducted. The difference between groups for all three passwords was significant, χ^2 (2, n=39) $\geq$ 6.81, $p < .05$. The graph revealed a recency effect for all three password groups, that is, the more recent the password was used/created the greater the accurate recall.

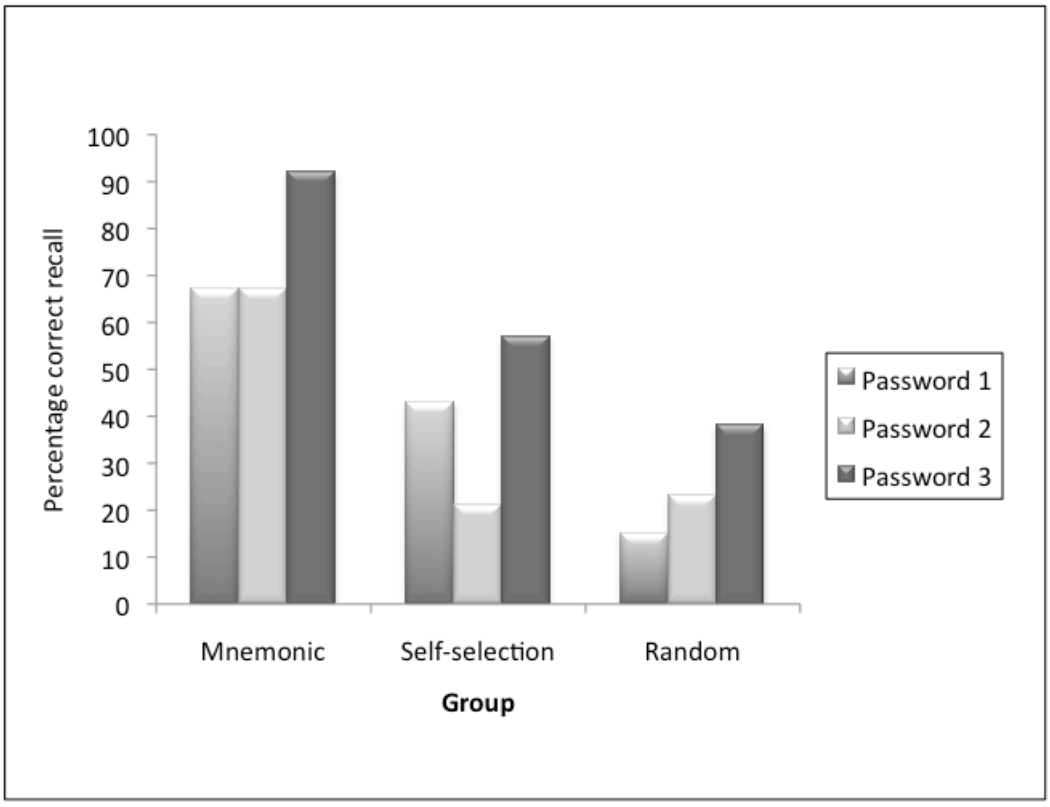


Figure 10. Percentage correct recall of all three passwords, for each group, at the conclusion of the study. Average response rate, 76 percent.

3.4 Password Strength

Password strength was calculated by measuring three items, *character length*, *alphabet size*, and *entropy*. Password strength was calculated for the mnemonic and self-selection groups only. Random passwords, allocated to the random group, should have a high degree of entropy, as they were randomly generated, thus security strength was analysed only for self-generated passwords. The minimum character length required per password was eight; therefore character length was scored as one point for eight characters and an additional point for each extra character. Alphabet size was scored as one point each for the following alphabet categories: password contained letters, password contained numbers, password included special characters, and password contained a combination of upper and lower case.

Entropy is a measure of disorder or randomness and is scored subjectively. In the present experiment, three parties rated the entropy of the passwords using a scale of 0 – 5: Zero was given if the password did not meet the initial requirements set out on the instruction sheets (for example, some participants used complete words in their passwords), and 5 was allocated for a high degree of apparent randomness. The three raters' scores were fairly similar, for the mnemonic group the mean ratings were (M = 3.29, SD = .91), (M = 4.33, SD = .86), (M = 4.43, SD = .63), and for the self-selection group the ratings from the three raters were (M = 3.2, SD = 1.47), (M = 3.2, SD = 1.56), (M = 2.22, SD = 1.60). The following are examples of passwords that received a high score on entropy:

- ss7ga830&dh
- 1sf8g1n08
- pcht05jc
- 1ha9ma7sh8ti
- wh&t4rs&fj

Some examples of passwords that received a low score on entropy:

- Bl8ue8bo8x
- im21@1986
- emosneve8
- Princess2
- draunbi08

The scores for all three measures (length, alphabet size, and entropy) were totalled to create an overall password strength score for each password created. The mean scores for each variable, for both groups, can be seen in Figure 11. The overall password strength for mnemonic and self-selection passwords generated in the study and the 95% confidence intervals can be found in Figure 12. The findings imply that participants in the mnemonic group were able to create passwords that were stronger (more secure) overall than the self-selection group.

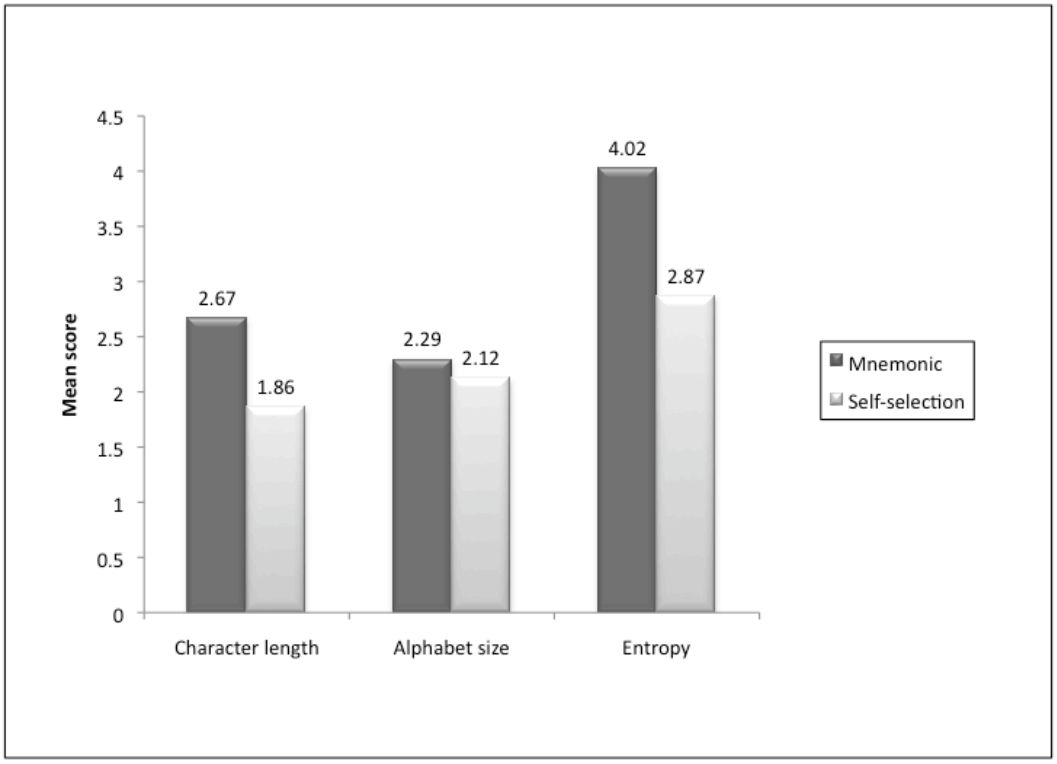


Figure 11. Mean score for password strength as a measure of character length, alphabet size and entropy.

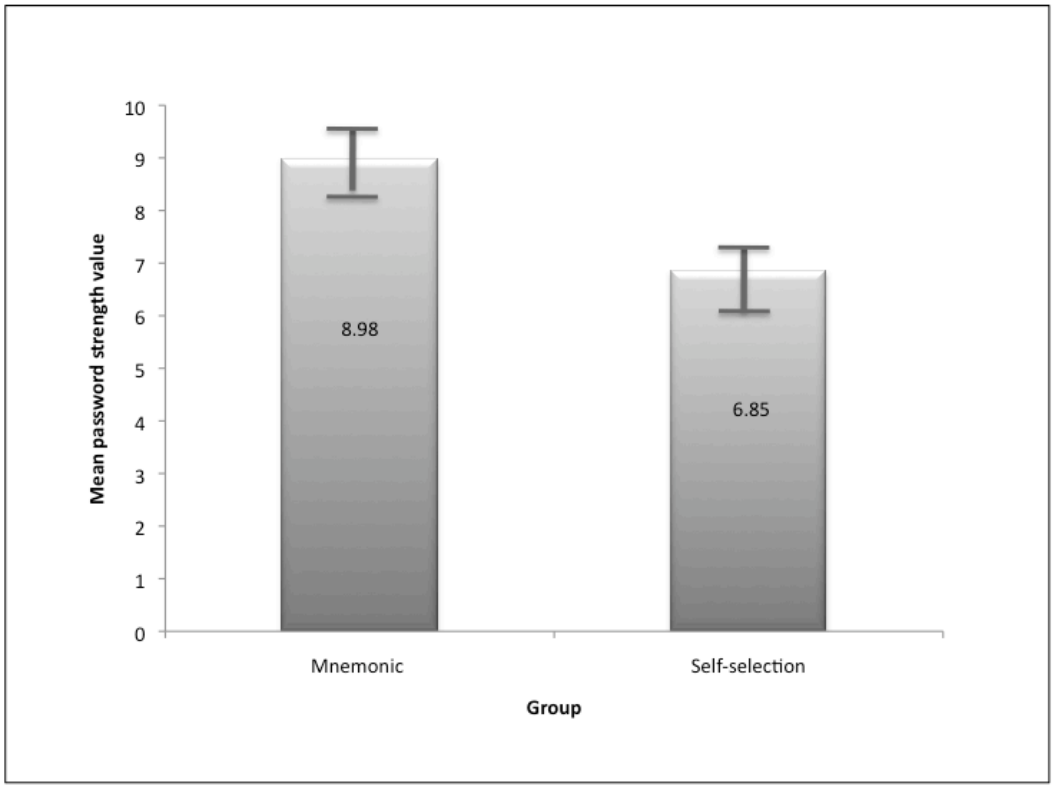


Figure 12. Mean security strength of passwords for the mnemonic and self-selection groups, a function of character length, alphabet size, and entropy. The vertical bars represent 95% confidence intervals.

3.5 Incorrect Recall - Error Analysis

3.5.1 Mnemonic group

Looking back at the percentage correct recall of passwords in Figure 7 we can see a decrease in correct recall for the mnemonic group from password 1 to password 2. Which later corrected itself in password 3. A repeated measures t-test was carried out to ascertain whether the decrease in correct recall was significant. The change was not significant, $t(16) = .89$, $p > .05$ between password 1 and password 2, and not significant between password 2 and password 3, $t(16)= -1.51$, $p > .05$. The difference in recall of password 1 and password 3 was also examined and found to be not significant, $t(16) = -.62$, $p > .05$

Although the statistical data show that the decrease in password recall between password 1 and 2 was not significant, statistical difference is not always practical difference. For the purpose of this study, reasons for the decrease in

accurate password recall for the mnemonic group were examined further to provide insight into why the errors occurred, and if possible, how they may be corrected. Five participants within the mnemonic group incorrectly recalled a password. Figure 13 portrays a summary of the error analysis.

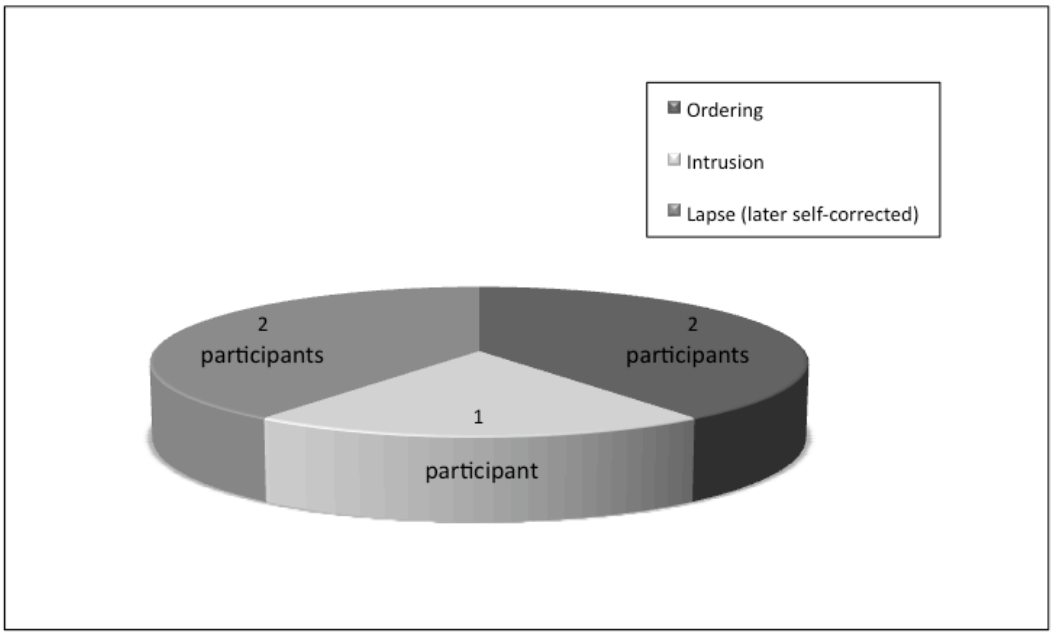


Figure 13. Number of participants in mnemonic group that incorrectly recalled a password, and the type of error made.

A *lapse* occurred when the participant was unable to correctly recall the password at the current recall attempt, yet they were able to later correctly recall the password at a following trial. One participant experienced an *intrusion* (an intrusion is usually an answer that would be correct in another context, Deese, 1959) in their password when they added another variable to their item list. That is, the participant chose 'friends' as their category heading, then listed three friends (first names) and their respective ages. At recall time they correctly listed the friends and their ages in order, but also added the initial from the friend's surnames. English was not the first language of the participant. It is not known if this may have contributed to the error. Finally, an *ordering* error occurred when the participant correctly recalled the password but entered the items in the incorrect order. For one participant, the ordering error may have been due to the password category chosen being the same as the previous password. All, save one,

of the participants who incorrectly recalled a password, failed to follow the steps laid out in the instruction sheet. However, they acknowledged this at the following password renewal meeting and completed all steps when creating password 3. The results show how performance improved again when participants in the mnemonic group selected their third password (see Figure 6).

3.5.2 Self-selection group

Failure to accurately recall passwords, for participants in the self-selection group, appeared to be due to many and various reasons, and some types of errors occurred simultaneously. Still, there were some consistent mistakes carried out, they included: mixing upper and lower case, using the wrong number, ordering problems, missing out items, and intrusions. Figure 14 represents the percentage and types of errors made by the self-selection group. In all, 12 participants in the self-selection group incorrectly recalled a password, with six of those participants incorrectly recalling more than one password.

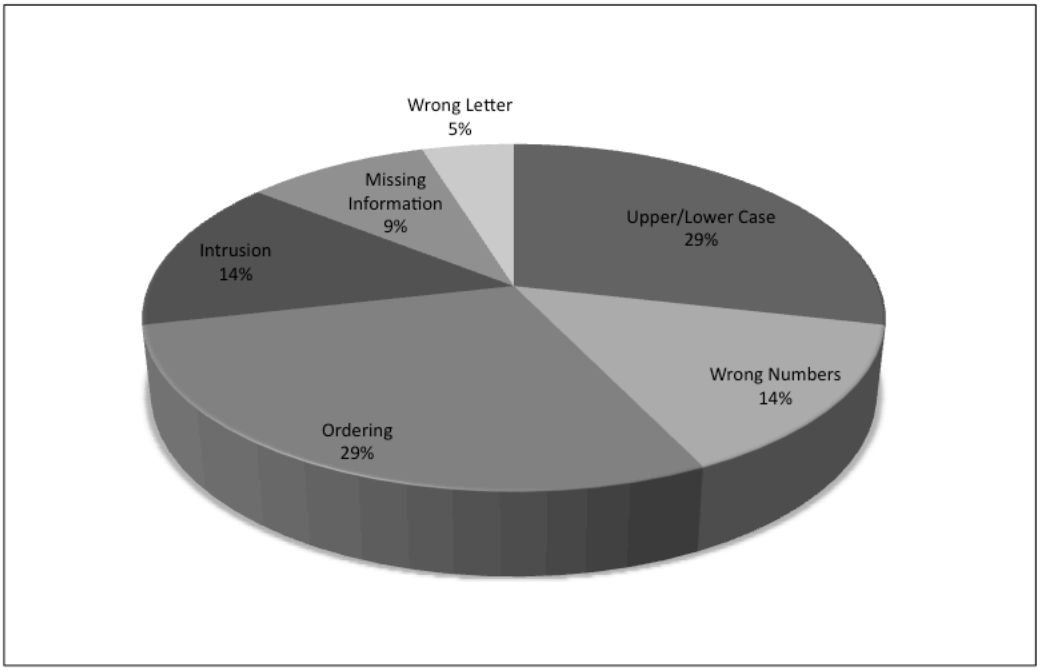


Figure 14. Types and percentages of password recall errors made by participants in the self-selection group.

3.5.3 Random group

Incorrect password recall also occurred within the random group for many and varied reasons, and it was at times difficult to determine the type of error that was occurring. However, there were some consistent mistakes carried out, they included: ordering difficulties, intrusions, only remembering the salient information, wrong or missing numbers, wrong letters, and getting the password entirely wrong. Figure 15 shows visually the types and percentages of recall errors made by participants in the random group. In total, 15 participants in the random group incorrectly recalled a password, with 10 of those participants incorrectly recalling more than one password.

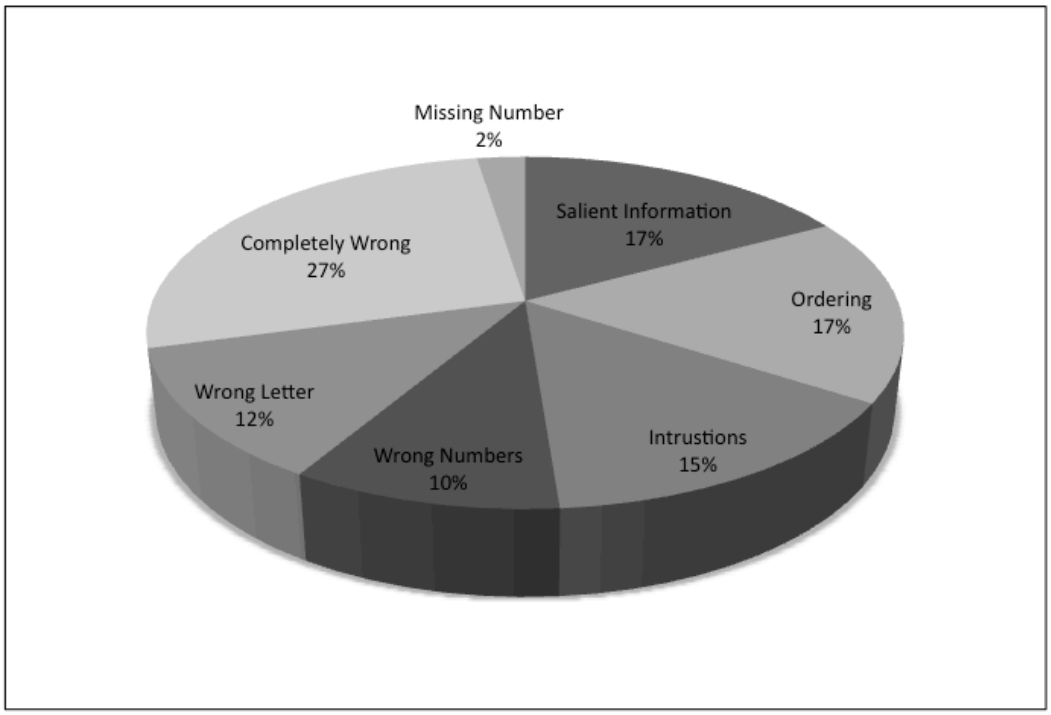


Figure 15. Types and percentages of password recall errors made by participants in the random group.

3.6 Subjective Findings

3.6.1 Mnemonic group

Seventy-five percent of participants in the mnemonic group who completed the post study questionnaire (response rate was 71%) volunteered that

the password cue helped with password recall. As seen in Figure 16, all participants in the mnemonic group found their passwords ‘easy’ to remember. Table 4 shows some of the comments made by participants in the retrospective post-study questionnaire, regarding the study.

Out of the participants who completed the online post-study questionnaire, three of them said, ‘yes’ earlier passwords did interfere with remembering the new password. Yet, two of those participants had 100 percent accurate recall over all trials, including the retrospective post-study password recall. The remaining participant was correct on all passwords trials (including post-study), except for one password.

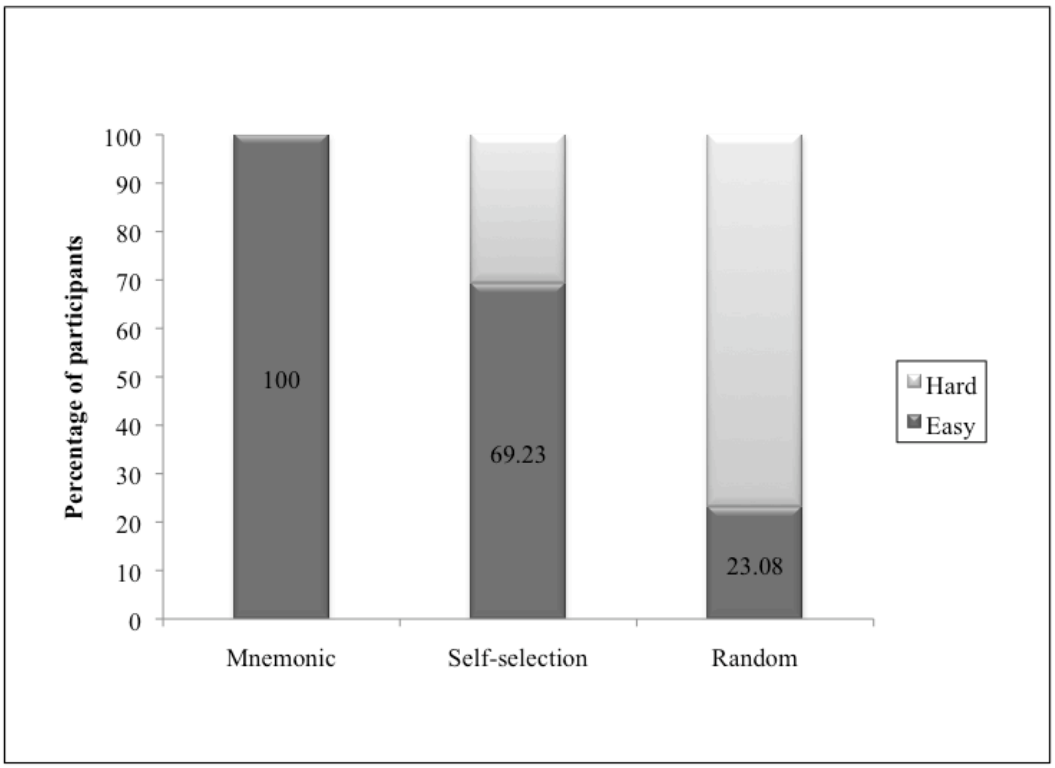


Figure 16. Percentage of participants in each group, who completed the retrospective post-study questionnaire, who perceived their passwords as ‘easy’ or ‘hard’ to remember.

Table 4

Some comments from participants in the mnemonic group, about the study, recorded in the retrospective post-study questionnaire

○ They related to something I knew. The cue triggered the sequence I needed to remember.
○ The password was always related to a topic I was familiar with, so even if I was struggling to remember at time the keyword always triggered the memory.
○ Just remembered them by the way we created them.
○ I couldn't believe how easy it was to remember. The hard part was coming up with the password itself.
○ It really made me think about the passwords I do use, which could probably be easy to hack, and how easy it is to make a complicated password easy to remember.
○ Should be used in all workplaces, training staff etc.
○ I will now apply this practice to remember passwords in the future.

3.6.2 Self-selection group

Participants in the self-selection group were not given any direction when creating their passwords, just the criteria for what the password must or must not include. Yet many people applied their own personal system of password creation. We asked participants about the method that they used in the post-study questionnaire. A summary of the systems used is shown in Figure 17. The response rate for the post-study questionnaire for participants in the self-selection group was 82 percent.

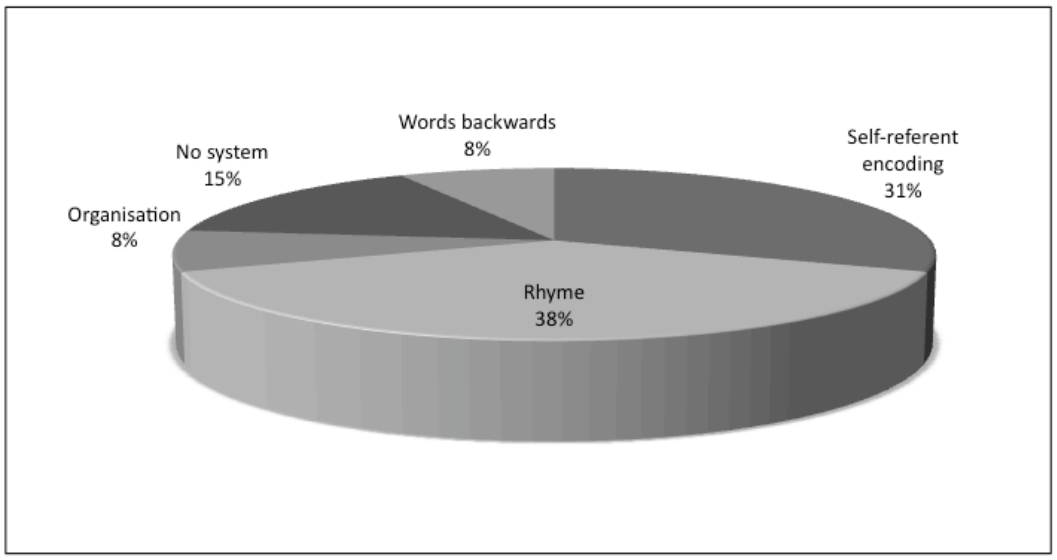


Figure 17. Password systems used/created by participants in the self-selection group, to assist with password recall.

Self-referent encoding applied to participants who used something familiar to them to create their passwords. Many used a rhyme, saying or song to go with the password. One participant mixed the names of two people and added a birthday to the end, using both self-referent encoding as well as organisation. Another participant used complete words backwards with numbers in-between (they found the word easy to recall but had trouble remembering which numbers they had used). A number of participants in the self-selection group used one or more of the memory tools applied in the mnemonic group, but did not utilise all the rules together. Table 5 shows some of the comments made by self-selection participants in the retrospective post-study questionnaire, regarding the study. For the question "Did any of your earlier passwords interfere with remembering your new password?" only one participant in the retrospective post-study questionnaire, for the self-selection group, answered 'yes'.

Table 5.

Some comments from participants in the self-selection group, about the study, recorded in the retrospective post-study questionnaire

○ I reckon it was a good exercise, timely with the use of internet passwords in our intranet websites, bank, mobile and email account....
○ Was easy to participate - would be easier if could remember passwords!!!
○ Hope you get what you are wanting from it
○ I had them (*the passwords)* as complete words backwards with numbers in-between. I could easily remember the letters, but sometimes had trouble remembering which numbers I had used and where I had put them
○ Tried to remember them *(the passwords)* in my memory – by associating them with something familiar to me, i.e. song

3.6.3 Random group

Participants in the random group were also asked if they applied some system to remembering their passwords. Figure 18 portrays the types of methods used by the participants. The response rate for the post-study questionnaire for participants in the random group was 76 percent.

Many in the random group used a method of associating the password with either real words, something familiar to them, or making up a sentence to fit the allocated password. Some broke the password into chunks to aid recall. Other participants used maintenance rehearsal, which is a form of rote repetition of the password until they thought they were able to remember it. Table 6 shows some of the comments participants in the random group made in the retrospective post-study questionnaire, regarding the study. Four participants in the random group (who participated in the post-study questionnaire) said, ‘yes’ they felt that old passwords did interfere with remembering the current password.

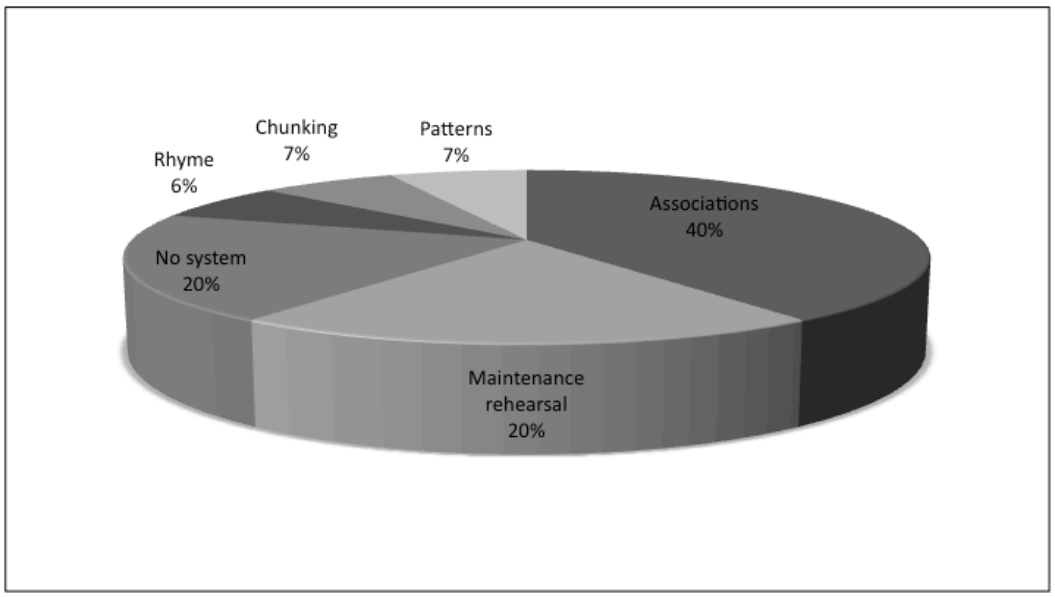


Figure 18. Types of password systems used by participants in the random group, to assist with password recall.

Table 6.

Some comments from participants in the random group, about the study, recorded in the retrospective post-study questionnaire

○ If the randomly given password is for an important website or personal account, I will make effort to remember it. But if not, I can easily forget it. Furthermore, if I was given more than 2 randomly selected passwords at the same time, it'd be frustrated for me to recite them. In addition, as below, if a new password is given, the older one can't be remembered.
○ Yeah once it is over it is over, can I recall them now, I doubt it. I saw it as a self competition as well, was determined to recall them. I cannot recall at all number 2 but if I had a starter Id be away....
○ I'd love to find out your method you've worked out, to find out if I could use it, cause I'm really not keen of the current method I have which is whole words and relating numbers.
○ Memorized my first one (password) by relating the letters and numbers to something familiar to me. The second and third ones were harder to relate to something so I forgot them almost straight away.
○ Recited them (*passwords*) over and over in my head constantly until they were stuck in

3.7 General Findings

Figure 19 depicts the type of password usually created by participants. As can be seen, a mixture of complete words and numbers is the most common type of password used. Passwords in the 'other' column include passwords assigned on entry to a system, nonsense words, a poem, or all numbers.

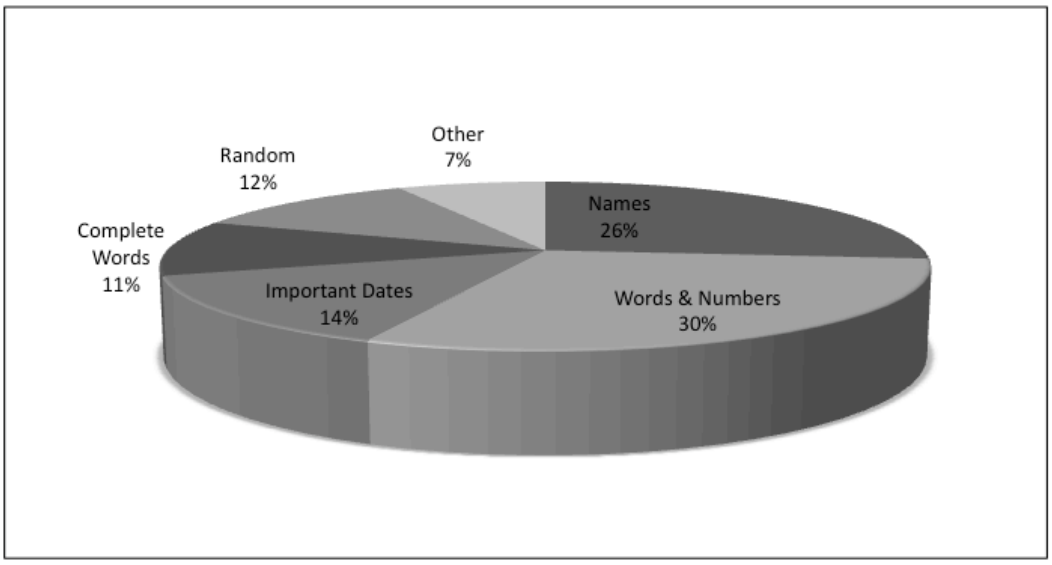


Figure 19. Type of password most commonly created by participants. Based on information provided in the background questionnaire.

Eighty-eight percent of participants were asked (on average, at two sites) to renew their password as various intervals, mostly every 60 days. An interesting occurrence, although maybe not surprising, was that many participants (sometimes across trials) were unable to enter the correct user name, even though the user name was clearly shown in the recall email sent out weekly (seen in Figure 4), alongside the link to the login page. Some participants used their personal or work email user names, their names on their own, or an incorrect version of their user name.

3.8 Summary of the Results

The results obtained across the study showed that the mnemonic group was significantly different from the self-selection and random groups. Accurate recall for the mnemonic group was superior in terms of: significantly more

accurate recall across all three passwords, visibly less attempts at entering a correct password, at each recall trial, and superior recall of all three passwords at the conclusion of the study.

With regard to password strength and security, both self-selection and mnemonic passwords were tested on the basis of password character length, alphabet size, and entropy. The findings indicated that participants in the mnemonic group created passwords that were stronger overall than passwords created by the self-selection group.

Error analyses for all three groups revealed a similar pattern of mistakes, with ordering errors, intrusions, missing numbers and letters, and mixing-up upper and lower case. However, participants in the mnemonic group were able to self-correct their mistakes by going back to following the instructions provided. The subjective findings from the retrospective post-study questionnaire revealed the systems used by participants in the self-selection and random groups to aid with password recall. They included self-referent encoding, the use of rhymes and organisation for the self-selection group, and the use of associations, chunking, and maintenance rehearsal for the random group.

The post-study questionnaire also showed that all participants in the mnemonic group found their passwords easy to remember, while two thirds of participants in the self-selection group found their passwords easy to remember and less than a third of participants in the random group found their passwords easy to remember. This information was complemented by the comments made about the study by participants in each group.

4. Discussion

The system of password generation, incorporating a variety of mnemonic aids, presented in this study was found to be useable, secure and memorable. This was revealed in a number of ways. Firstly, participants in the mnemonic group were able to accurately recall all three passwords, across the three trials for each password, significantly more than participants in the self-selection and random groups recalled their passwords. The ability to remember the passwords, was not only more accurate at each trial, but long-term memory of the passwords remained stronger for the mnemonic group, this was revealed in the retrospective post-study questionnaire where recall of all three passwords was performed. These results are in direct contrast to those found by other studies carried out in this area. In particular, Henry (2007) who tested a variety of password generation systems, mainly passphrase based, across a similar timeframe, found an overall recall rate of 30 percent. Lu and Twidale (2003) also tested a system that provided password and login cues, however the recall rate was similar to the self-selection group in this experiment, sitting at around 65 percent accurate password recall.

The number of attempts used at each password trial also indicated how memorable the passwords generated by the mnemonic group were, and may also be an indication of participant motivation. Given that, if the participant was unable to recall their password, they were less likely to attempt to recall the password at a later stage or give up after one or two attempts. Vu et. al. (2007) has suggested that the 'three times and you're out' rule for password entry is too severe. They propose that if the number of attempts allowed was increased, accurate recall may increase. Yet, the mnemonic group in this study, on the whole, only needed one attempt to gain a 'correct – thank you for participating', which confirms that the passwords created by them were memorable.

Passwords created by the mnemonic group were more secure than passwords created by the self-selection group, as the passwords generated had a greater number of characters in them, slightly higher alphabet size, and a higher degree of entropy. If we assess the passwords produced on the basis of password

strength described in the introduction (section 1.2) they may be somewhat deficient in the area of alphabet size. All the passwords created by the mnemonic group included letters and numbers, however only some included special characters, and a few utilised upper and lower case. One way to improve alphabet size, would be educating users on what a strong password consists of, providing information on the effect of character length, alphabet size and entropy, on password security. Participants in this study were not provided with any information on password strength. However, the character length and degree of entropy of the passwords generated by the mnemonic group suggests that they are relatively safe from guessing attacks.

Assessing whether the mnemonic system applied in this study was usable requires a more indirect approach. Usability can be revealed in the performance of a system, yet it is also a perception of the user. From information collated in the post-study questionnaire, we can see that all participants in the mnemonic group (who completed the questionnaire) found their passwords 'easy' to recall. This was supported by the comments made by participants in the group. For example, "…how easy it is to make a complicated password easy to remember", "The password seemed logical…", "Applying rational, logical order worked for me…", "I couldn't believe how easy it was to remember". Another sign of usability is the number of trials missed or not attempted, as noted previously, this may be an indicator of participant motivation. Weirich and Sasse (2002) put forward that "password mechanisms and their users form a socio-technical system, whose effectiveness relies strongly on users' willingness" to engage in the process (p. 137). The results showed that the mnemonic group had six trials which were not attempted, compared to twice that many for the self-selection group, and 14 trials missed by participants in the random group. Overall, the mnemonic system used here appears to be usable.

The occurrence of password renewal had an interesting effect on recall results. In Figure 6 we see that changing passwords had little effect on the performance of the random group, accurate recall remained just below 50 percent for all three passwords. For the self-selection group accurate recall dropped when the password was initially changed, and then dropped slightly again when the password was renewed for the third time. Password recall for the mnemonic group

looked extremely positive for the initial password, only one participant failed to recall their password, and this was due to interference. Yet when the first password change occurred at week four, three participants were unable to recall their passwords. The errors appeared to be due to ordering problems (two participants) and a lapse for one participant. All three of these participants took a shortcut during the generation process. Weirich and Sasse (2002) reiterate that most users will cut corners to reduce task load. This indicates that the cognitive encoding processes involved in the generation stage do have an effect on recall. This is looked into further later in the discussion. For the third and final password change, recall for the mnemonic group rose back up to nearly 100 percent accuracy, just one participant incorrectly recalled their password in the second trial $R_{(3\text{-}2)}$ and later self-corrected it in the third trial $R_{(3\text{-}3)}$. The low failure rate for the mnemonic group is exceptional when compared to other studies. Lu and Twidale (2003), using a Minimal Feedback Authentication (MiFA) system, that revealed parts of the login and password to participants, had 66 percent password recall, with a small sample, after one week delay. Henry (2007) tested 139 participants, who were technically adept, weekly, over seven weeks (which is more inline with this study), and found that only 30 percent of participants were able to correctly recall their passwords over the course of the study. Therefore we can confirm that incorrect password recall, when changing a password, was lower for the mnemonic group than the self-selection and random groups. We may also presuppose that incorrect password recall at renewal time is lower using this method than other methods available at this time.

Assessing whether, and to what degree, proactive interference occurred is more difficult. Participants were asked whether they felt the older passwords interfered with the password currently being recalled. The highest response came from the random group, with four participants stating ‘yes’, closely followed by the mnemonic group with three participants agreeing, interestingly enough only one participant in the self-selection group felt that old passwords had interfered with the current one. Of the three participants in the mnemonic group, who felt that proactive interference had occurred, two had 100 percent correct recall across all trials, including the post-study recall. The other participant only missed one password, out of all the trials. So, it appears that it was a perception of proactive

interference, rather than interference actually occurring. Conversely, you could presume that the self-selection group would encounter proactive interference, with the medium to high rate of incorrect recalls that occurred, and yet they didn't perceive that it had taken place.

Proactive interference could have contributed to the incorrect password recall for one participant in the mnemonic group who incorrectly recalled the second password (they were one of two participants who had ordering problems). The category that they chose was the same category as the first password, and the cue used was identical. However, it was only after trying various combinations of the correct password that they resorted to adding items from the first password. On the third password they chose a category that was entirely different from the first two. This, as reported previously, creates a release from proactive interference (if it actually occurred in the first case). Conversely recall errors could be attributed to cue overload – having more than one memory/password associated with a single cue (Watkins & Watkins, 1975). In sum, it is not conclusive that the amount of proactive interference was less for the mnemonic group compared to the self-selection and random groups. Yet, we can see that interference, decay and errors were significantly less for the mnemonic group compared to the other two groups.

Heading back to the topic of the effectiveness of encoding processes involved in the generation of mnemonic passwords used in the study, Figure 20 depicts a password created by one of the participants in the mnemonic group, indicating the mnemonic aids utilized throughout the process.

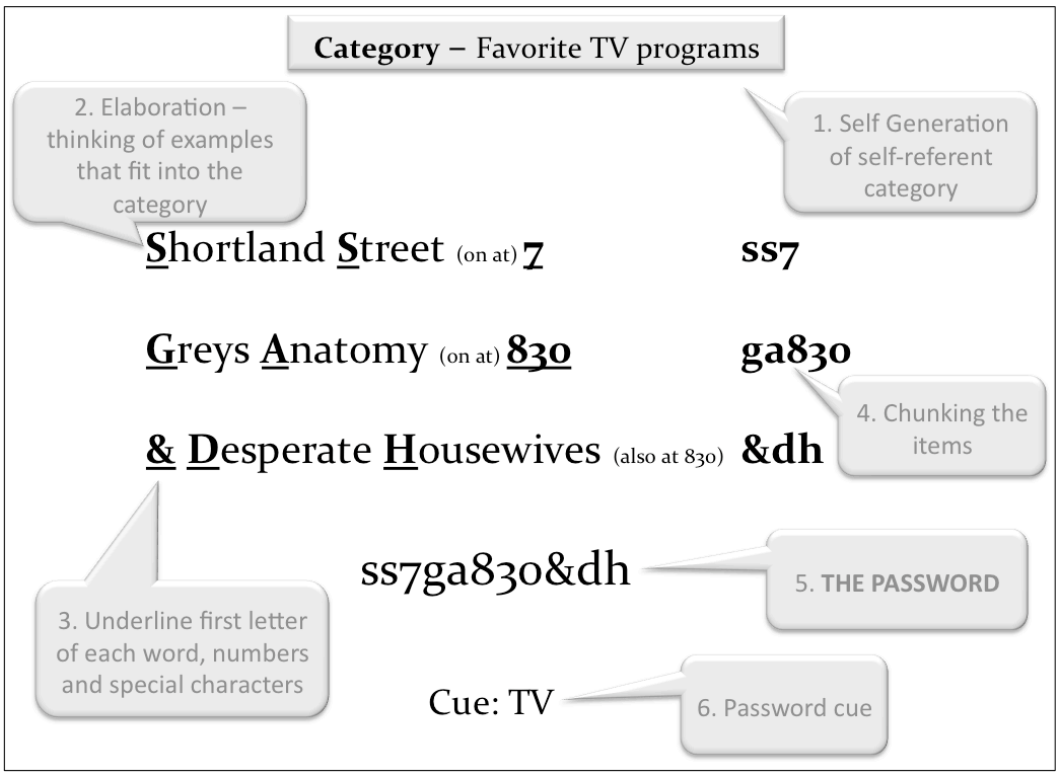


Figure 20. An example of a password created by a participant in the mnemonic group. The callouts indicate the mnemonic aids utilized and the order they occurred in the generation process.

The mnemonic aids used can be seen in the example, starting with the participant generating their own category heading of something that interests them or they have knowledge of (self-referent). Followed by elaborating on the theme and listing three or four items associated with the category. The first letters, any numbers or special characters were then underlined – this is similar to the sentence generation/pass phase methods used by other researchers. The characters underlined were then taken to the side and chunked into a single unit for each line. The complete password was then written below, while the participant repeated to himself or herself what each character stood for. Finally, the cue was recorded and later used as a reminder/prompt when the login email was sent to participants in the mnemonic group (see Figure 4).

In order to understand whether all or only some of the mnemonic aids were necessary, we can look back at the errors that occurred as well as the comments made by participants in the post-study questionnaire. Regarding the password cue, three quarters of participants in the mnemonic group of their own accord, said that the cue helped with remembering their password, as seen from the following comments by participants: “The cue triggered the sequence I needed to remember…”, “…even if I was struggling to remember at times the key word always triggered the memory”. The cue appeared to have worked like a door handle, once turned it opened the door to the complete password. Participants in the mnemonic group also reported that because the items were self-referent it helped them to remember them, or to put it in their own words, “They related to something I knew…”, The password was always related to a topic I was familiar with…”, “because it was related to something I knew well, it was easy to remember because it wasn’t a random assortment of some numbers and letters it had some meaning”. This information suggests that passwords that are self-generated, using material that is personally meaningful, facilitates recall. Chunking the first letter of the items listed meant that only three units needed to be remembered rather than eleven characters, this would reduce task workload, and therefore assist with recall. From the error analysis, we saw that participants who failed to follow the steps shown in Figure 20 had difficulties with password retrieval. Therefore we could assume that the process of writing down the category items, then listing the chunks, followed by writing the complete password down, does have an effect on the ability to accurately recall the password. So, it appears that all the mnemonic aids used in the present study do have a function and role in the accurate recall of passwords.

The practical implications of this study are promising. The mnemonic system demonstrated here could be applied to many password applications, particularly where information security is paramount. However, education about the types of attack passwords are vulnerable to and the characteristics of a secure password should be taught in conjunction with the system, to provide an understanding of why secure password systems are necessary and to increase user compliance. A limitation of the present study, though, is that it only tested a single password at a time, it would be of interest to see the effects of testing multiple

passwords concurrently using the same mnemonic system. For example, participants could begin by generating a single mnemonic password, tested across a period of weeks then additional passwords could be added at certain points, while retaining the previous passwords. Of interest, would be the effect of categories used, that is; do the category headings used as a basis for the password items need to be mutually exclusive? And at what point do passwords begin to interfere with one another? An unexpected finding, in the present study, was that many participants were unable to correctly enter their user name on the login page, even though it was clearly stated on the reminder email (seen in Figure 4).

A suggestion to cope with these potential difficulties – that is using multiple accounts with multiple passwords and usernames – would be creating a password organiser that looks like the chart in Figure 21. As can be seen, a single password was applied to multiple sites, this could be acceptable if the password chosen was strong, and the important sites had their own unique password.

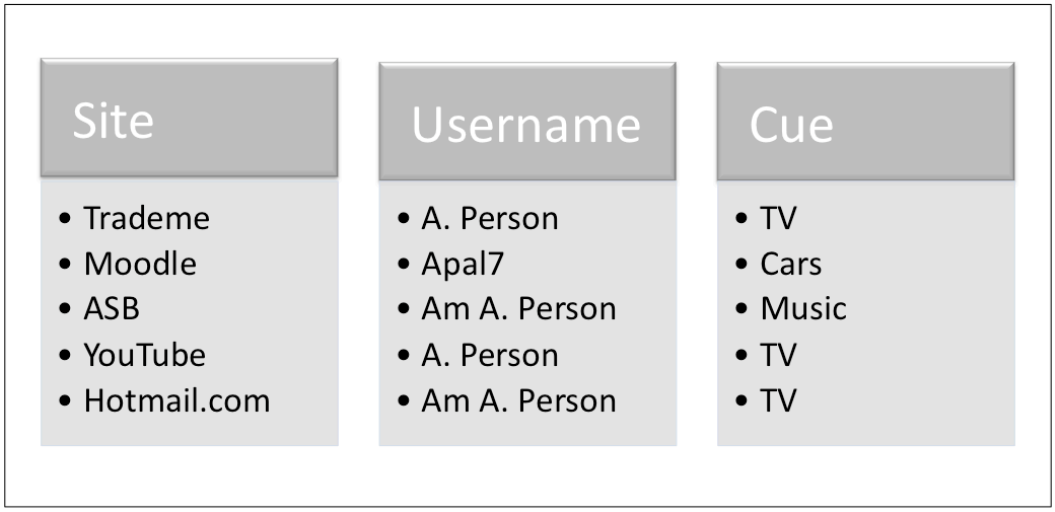


Figure 21. Password organiser, showing the application site, username and password cue (note some passwords are used at multiple sites).

In conclusion, the present study showed that there is hope yet for passwords. Using mnemonic processes enabled participants in this sample to accurately recall their passwords nearly 100 percent of the time. This is a dramatic

increase compared to results from previous research in this area. Ultimately, the system presented here needs to be tested in the market place, and applied to multiple applications, with multiple passwords at the same time, in conjunction with user education, in order to see how it stands up in the ‘real world’.

References

Anderson, J.R. (1976). *Language, memory and thought.* New Jersey: Lawrence Erlbaum Associates.

Andrews, L.W. (2002). Passwords reveal your personality. *Psychology Today, 35*(1), 16.

Austin, J. (1813). *Pride and Prejudice (3rd ed, 1991).* London: Tiger Books International.

Beal, C.R. (1985). Development of knowledge about the use of cues to aid prospective retrieval. *Child Development, 56*(3), 631 – 642.

Bjork, R.A., & Whitten, W.B. (1974). Recency-sensitive retrieval processes in long-term free recall. *Cognitive Psychology, 6,* 173 – 189.

Brown, A.S., Bracken, E., Zoccoli, S., & Douglas, K. (2004). Generating and remembering passwords. *Applied Cognitive Psychology, 18,* 641-651.

Campbell, J., Kleeman, D., & Ma, W. (2007). The good and not so good of enforcing password composition rules. *Information Systems Security, 16,* 2 -8.

Chase, W.G., & Simon, H.A. (1973). Perception in chess. *Cognitive Psychology, 4*(1), 55 – 81.

Craik, F.I., & Lockhart, R.S. (1972). Levels of processing: A framework for memory research. *Journal of Verbal Learning and Verbal Behavior, 11,* 671-684.

Deese, J. (1959). On prediction of occurrence of particular verbal intrusions in immediate recall. *Journal of Experimental Psychology, 58*(1), 17 – 22.

Ferguson, N., & Schneier, B. (2003). *Practical cryptography.* Indianapolis, Indiana: Wiley.

Gaw, S., & Felten, E.W. (2006). Password management strategies for online accounts. *ACM International Conference Proceeding Series, 149*, 44-55.

Gobet, F., Lane, P.C.R., Croker, S., Cheng, P.C-H., Jones, G., Oliver, I., & Pine, J.M. (2001). Chunking mechanisms in human learning. *Trends in Cognitive Sciences, 5*(6), 236 – 243.

GoedSoft. (2005). Good and bad passwords. How-to. Available:

http://geodsoft.com/howto/password/cracking_passwords.htm.

Goggin, J., & Wickens, D.D., (1971). Proactive interference and language change in short-term memory. *Journal of Verbal Learning and Verbal Behavior, 10*(4), 453 – 458.

Granger, S. (2001). *Social engineering fundamentals, part 1: Hacker tactics.* Availability: http://www.securityfocus.com/infocus/1527. Downloaded August, 1 2008.

Groves, J. (2002). Truffles – myth or strategic plan? Sniffing out some bizarre and inspired ways of motivating people to remember their passwords. *Computer Fraud & Security, 1*, 9-12.

Harada, Y., & Kuroki, K. (1996). A study on the attitude and behavior of computer network users regarding security administration. *Reports of National Research Institute of Police Science, 37,* 21 – 33.

Henry, P.T. (2007). 'Toward usable, robust memometric authentication: An evaluation of selected password generation assistance'. Unpublished doctoral dissertation, Florida State University, College of Information, United States.

Horowitz, A.S. (2001). Top 10 security mistakes. *Computerworld, 35*(28), 38.

Jeyaraman, S., & Topkara, U. (2005). Have the cake and eat it too – infusing usability in text-password based authentication systems. *Proceedings of the 21st Annual Computer Security Applications Conference.*

Klein, S.B., & Loftus, J. (1988). The nature of self-referent encoding: The contributions of elaborative and organizational processes. *The Journal of Personality and Social Psychology, 55*(1), 5 – 11.

Klein, D. (1990). "Foiling the cracker": A survey of, and improvements to, password security. *Proceedings of the USENIX UNIX Security Workshop*, Portland, Oregon.

Lea, G. (1975). Chronometric analysis of the Method of Loci, *Journal of experimental psychology. Human perception and performance, 104*(2), 95 – 104.

Leonhard, M.D. (2006). *A comparison of three random password generators*. College of Engineering, University of Illinois at Chicago. Availability: http://tamale.net/coursework/cs398/leonhard.pwdgens.cs398.pdf

Leyden, J. (2003). Office workers give away passwords for a cheap pen. The

Register. Availability: http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/. Downloaded July 29, 2008.

Lu, B., & Twidale, M.B. (2003). Managing multiple passwords and multiple logins: MiFA minimal feedback hints for remote authentication. In M. Rauterberg et. al. (Eds). *Human-Computer Interaction* (p. 821 – 824). IOS Press, IFIP.

Miller, G.A., Galanter, E., & Pribram, K.H. (1960). *Plans and the structure of behavior*. New York: Holt, Rinehart, Winston.

Nairne, J.S. (2002). Remembering over the short-term: The case against the standard model. *Annual Review of Psychology, 53,* 53 – 81.

Paivio, A. (1965). Abstractness, imagery, and meaningfulness in paired-associate learning. *Journal of Verbal Learning & Verbal Behavior, 4*(1) 32 – 38.

Rogers, T.B., Kuiper, N.A., & Kirker, W.S. (1977). Self-reference and the encoding of personal information. *Journal of Personality and Social Psychology*, *35*(9), 677 – 688.

SafeNet, (2005). Results of Second Annual Global Password Survey Availability: http://findarticles.com/p/articles/mi_m0EIN/is_2005_March_7/ai_n11850986 Downloaded July 29, 2008.

Sasse, M.A., Brostoff, S., Weirich, D. (2001). Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19,* 122 – 131.

Slamecka, N.J., & Graf, P. (1978). The generation effect: Delineation of a phenomenon. *Journal of Experimental Psychology: Human Learning and Memory, 4*(6), 592 – 604.

Thorndike, E.L. (1911). *Animal Intelligence (Vol. 2)*. New York: Macmillan.

Topkara, U., Atallah, M.J., & Topkara, M. (2007). Passwords decay, words endure: Secure and re-usable multiple password mnemonics. *Security Applications Conference*, Seoul, Korea.

Underwood, B.J. (1964). Degree of learning and the measurement of forgetting. *Journal of Verbal Learning and Verbal Behavior, 3*, 112-129

Vu, K.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B., Cook, J., & Schultz, E.E.

(2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65,* 744 – 757.

Watkins, C., & Watkins, M.J. (1975). Buildup of proactive inhibition as a cue-overload effect. *Journal of Experimental Psychology: Human Learning and Memory, 1,* 442 – 452.

Wechsler, D. (1997). *WAIS-III Administration and Scoring Manual.* New York: The Psychological Corporation.

Weirich, D., & Sasse, M.A. (2002). Pretty good persuasion: A first step towards effective password security in the real world. *Proceedings of the 2001 Workshop on New Security Paradigms*, Cloudcroft, New Mexico.

Yan, J.J. (2001). A note on proactive password checking. *Proceedings of the 2001 workshop on new security paradigmes*. Cloudcroft, New Mexico.

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *Ieee Security & Privacy, IEEE, 2*(5), 25 – 31.

Yapp, P. (2001). Passwords: Use and abuse. *Computer Fraud & Security, 9*, 14.

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Appendix A

Welcome to the Internet Password Study

Instructions

The purpose of the study is to find out more about the practices of individual's with regard to Internet passwords, and to look at the generation and memorability of different types of Internet passwords.

We are asking participants in the study to:

1. Answer a questionnaire about their Internet password habits.
2. Complete a brief working memory test.
3. Generate or be assigned a password. You will be asked to enter your email address on a computer screen and enter the created password into the space provided (like a login page).
4. A week after the initial meeting you will be sent an email with a link to a webpage where you will be asked to enter your email address and password into the space provided. You will be given three tries at entering a correct password. You will be sent emails two and three weeks after the initial password was assigned or created, requesting you enter your password.
5. Three weeks after the initial meeting we will meet with you again to renew your password in the same way that the initial password was chosen. For the following three weeks you will be sent an email each week asking you to enter your renewed password.
6. We will then meet with you, for your password to be renewed for the third and final time. For three weeks after that you will be sent an email each week requesting your email address and password.
7. At the end of the study you will be emailed a brief questionnaire to complete online.

All information will be treated in the strictest confidence and if you have any questions feel free to ask us. You can withdraw from the experiment at any time.

We would like to begin by having you complete an informed consent sheet and then answer some background questions about your internet password habits.

Thank you in advance for your participation.
Tracy Filmer-Clark
filmer@wave.co.nz

Appendix B

University of Waikato
Psychology Department

Consent Form

RESEARCHER'S COPY

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Research Project: **Internet Passwords**

Name of Researcher: Tracy Filmer-Clark Name of Supervisor: Dr. S.G. Charlton

I have received an information sheet about this research project or the researcher has explained the study to me. I have had the chance to ask any questions and discuss my participation with other people. Any questions have been answered to my satisfaction.

I agree to participate in this research project and I understand that I may withdraw at any time. If I have any concerns about this project, I may contact the convenor of the Research and Ethics Committee (Dr Robert Isler, phone: (07) 838 4466 ext. 8401, email: r.isler@waikato.ac.nz).

Participant's Name: _____ Signature: _____ Date:_____

University of Waikato
Psychology Department

Consent Form

PARTICIPANTS COPY

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Research Project: **Internet Passwords**

Name of Researcher: Tracy Filmer-Clark Name of Supervisor: Dr. S.G. Charlton

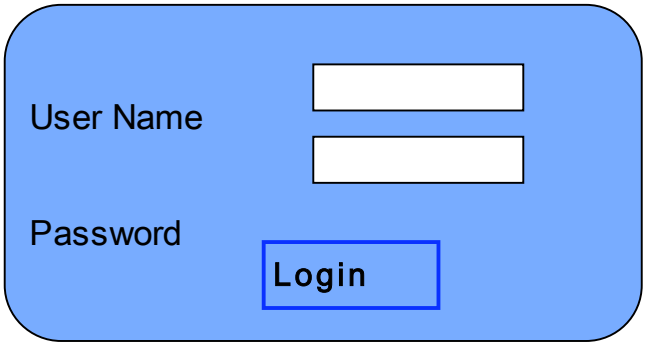
I have received an information sheet about this research project or the researcher has explained the study to me. I have had the chance to ask any questions and discuss my participation with other people. Any questions have been answered to my satisfaction.

I agree to participate in this research project and I understand that I may withdraw at any time. If I have any concerns about this project, I may contact the convenor of the Research and Ethics Committee (Dr Robert Isler, phone: (07) 838 4466 ext. 8401, email: r.isler@waikato.ac.nz).

Participant's Name: _____ Signature: _____ Date:_____

Appendix C

Participants Needed For Internet Password Study



We are asking participants in this study to:

- → Answer a questionnaire about your password habits.
- → Complete a brief working memory test.
- → Generate or be assigned a password, and enter into login page (like above).
- → A week later you will be sent an email and link asking you to login with your new password. This will be repeated two and three weeks later.
- → Then we will meet with you again to renew your password, and for the following three weeks you will be sent an email and link asking you to login with your new password.
- → We will then meet with you, for your password to be renewed for the third and final time. For three weeks after that you will be sent an email each week requesting you login with your latest password.
- → At the end of the study you will be emailed a brief questionnaire to complete online.

PSYC103 students will receive 2 course credits for taking part.
(as well as refreshments)

If interested, please txt me on
021 653 142
or email
filmer@wave.co.nz
Thanks, Tracy Filmer-Clark

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Appendix D

Background Questionnaire - Internet Password Habits

(all information provided will be kept in strict confidence)

1. Please tick the box for websites you use that require a password.

☐ ANZ	☐ email accounts	☐ Bebo
☐ ASB Bank	☐ For work	☐ Flixster
☐ BNZ	☐ Trademe	☐ MSN
☐ Kiwibank	☐ Ferrit	☐ Facebook
☐ National Bank	☐ Amazon	☐ YouTube
☐ TSB Bank	☐ iTunes	☐ Netlog
☐ Westpac	☐ Ticketdirect	☐ Online Games
☐ Other Banks	☐ Ticketek	☐ Other _____

2. How many different passwords do you use for these sites? _____
3. Do you write your passwords down? YES NO (circle one)
4. How many sites ask you to renew your password? _____
5. How often do you renew your passwords? (circle one)

   Weekly Monthly Every 60 Days Yearly Never

6. Have you ever forgotten a password? YES NO (circle one)
7. Have you ever contacted a 'help desk' to retrieve or reset a forgotten password? YES NO (circle one)
8. Please indicate what sort of password you usually choose:
   - □ Names (proper & nicknames)
   - □ Words & Numbers
   - □ Important dates
   - □ Complete words
   - □ Mixture of random numbers and letters
   - □ Other, please specify _____

9. Are you? Male Female (please circle)
10. How old are you? _____

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Appendix E
Retrospective Post Study Questionnaire

(all information provided will be kept in strict confidence)

Please circle which best applies to you, or write in the space provided

1. Did you later write any of your passwords down? Yes No (circle one)
2. Have you used your passwords anywhere else? Yes No (circle one)
3. How did you remember your passwords?

4. Were your passwords easy or hard to remember? Hard Easy (circle one)
5. Why do you think so?

6. Did any of your earlier passwords interfere with remembering your new password? Yes No (circle one)
7. Other comments you wish to make regarding the research

8. If possible, please recall your passwords in the space provided

   Password 1. _____

   Password 2. _____

   Password 3. _____

Thank you for participating in this study of password generation and memorability. If you wish to receive a summary of the results, please provide us with your email address: _____

THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

Appendix F

Internet Password Study

Participant Instructions

Self-Selection Group

You need to select a password. The password you choose must be between 8 – 12 characters long and include at least 1 letter and 1 number and may include special characters. Do not use a password that you use elsewhere and that you have used in the past.

Do not choose a password that can be easily guessed or that relates to known personal information about yourself and your family such as birthdays, names, or telephone numbers. Also do not use sequential numbers such as 4321 or repetitive numbers such as 4444. Do not use complete words.

Enter your email address on the screen, where requested. Once you have thought of your password enter the password into the space provided.

Do not share your password with anyone else.

Do not write down or record your password

Thank you for your time and your participation.

Appendix G

Internet Password Study

Participant Instructions

Random Group

Below is a random password between 8 – 12 characters long. Take a few minutes to memorise it then enter your email address on the screen, where requested and enter the password into the space provided.

9awfcevas

Do not share your password with anyone else.

Do not write down or record your password.

Thank you for your time and your participation.

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

Appendix H

Internet Password Study

Participant Instructions

Mnemonic Group

You need to select a password. The password you choose must be between 8 - 12 characters long and include at least 1 letter and 1 number and may include special characters. Do not use a password that you use elsewhere or that you have used in the past.

Do not choose a password that can be easily guessed or that relates to known personal information about yourself and your family such as birthdays, names, words or telephone numbers. Also do not use sequential numbers such as 4321 or repetitive numbers such as 4444.

Follow these steps in choosing your password:

1. Think of a category of something that interests you, for example, cars, a specific sport, a type of animal, colours, flowers, music etc.
2. Within this category think of three or four different items that fit into it. They can be more than one word and can also have a number in them.
3. List the items. If they do not include any numbers then add a number to the front or back of the item. Some examples are:

Cars	Music Bands
BMW Z3 (Roadster)	1. Foo Fighters
BMW 5 Series	2. Artic Monkeys &
BMW 7 Series	3. Led Zeppelin!
Audi A8	

Fishing (I caught…….)	Spring Flowers (I planted…)
2 Kahawai	30 Daffodils
4 Snapper	20 Tulips
6 Tuna	15 Iris
8 Striped Marlin	5 Freesias

4. Write the list again, this time thinking of and picturing the item as you write it. Then underline the first letter of every word and every number.
5. Say each line to yourself and then say the underlined letters and numbers continue with the next line, until finished. For example:

BMW **Z3** (Roadster)	**Z 3**		**1** **F**oo **F**ighters	**1 FF**
BMW **5** Series	**B 5**	**OR**	**2** **A**rtic **M**onkeys **&**	**2AM&**
BMW **7** Series	**B 7**		**3** **L**ed **Z**eppelin**!**	**3 LZ !**
Audi **A8**	**A 8**			
= z3b5b7a8			**= 1ff2am&3lz!**	
Cue: Cars			*Cue: Bands*	

6. Then write out the underlined letters and numbers and say to yourself, without looking at the full description. These letters and numbers are the password. Repeat these steps, if necessary, until the password has been learnt and can be repeated without looking at the paper.
7. On a separate piece of paper write the category heading, e.g. Cars to use later as a password cue.
8. Enter your email address on the screen, where requested. Enter the password you have created into the space provided.
9. Please hand in all paper you have used in the experiment. We will keep a record of your category heading for next time.

Further Examples

Television (My favourite programs are…….)

Dancing with the stars 1	**DWTS 1**
&	**&**
American Idol 2	**AI 2**
= dwts1&ai2	*cue: TV*

Rugby

Dan Carter 12	**DC 12**
Jo Rokocoko 14	**JR 14**
Richie McCaw 7	**RM 7**
= dc12jr14rm7	*cue: Rugby*

Do not share your password with anyone else.

Do not write down or record your password.

Thank you for your time and your participation.