Effect of password sentences with emotional content

Kirsi Helkala
Norwegian Defence Cyber Academy
khelkala@mil.no

Abstract

The usage of passwords as an authentication method does not show any sign of decreasing; to the contrary, passwords are used more than ever. In order to keep passwords secure enough to match assurance levels of the services users' knowledge has to be updated. Users' confidence to generate strong but still memorable passwords; password self-efficiency, can be increased by allowing full sentences to be used as login secrets. In this paper, we show the results of two independent experiments where full sentences were used as login secrets. The sentences which were used in these experiments had either positive or negative content. The sentences with positive content were remembered better than sentences with negative content in both experiments.

1 Introduction

Passwords are said to be old-fashioned but still they are used more than ever. According to the national password study [10] an average Norwegian adult has 25 passwords in use either as a single factor or as a part of a multi-factor authentication method.

It is not an easy task to remember 25 random-like passwords, and one of the weakness of passwords lays indeed in their memorability. In the beginning of the password history, a single word used as a login secret was acceptable, but now increased computing power makes them easy targets for offline attacks. Offline attacks are not as time consuming as they used to be, because of the usage of ready made password hash tables e.g. [24].

In order to be robust against attacks using the hash lists, the passwords should to be *much* longer and contain characters from all character sets: digits, lower case letters, upper case letters and symbols. One could therefore claim that these passwords would be harder to remember than earlier ones. However, this claim is not necessarily true.

Memory is one of humans cognitive abilities [22] and it is not easily understood. A person might remember long dialogues word by word far from the past and simultaneously cannot recall the name of the person he just met. The phenomena, called memory trade-off [17], is commonly known but still difficult to explain in depth.

This paper was presented at the NISK-2014 conference.

The research shows that there are several factors which affect person's cognitive abilities. Some factors have negative effect such as fatigue [7] and hunger [5]. Good physical condition [4] is an example of factors that affect positively. Some factors' effect depends on the circumstances. Environmental factors are examples of these [2]. Also feelings have an influence. The emotional arousal, either positive or negative, helps humans to maintain a readiness to respond [20] which helps us to notice and encode incidents or details around us.

In this paper, we study how emotional content of the password can be useful when designing strong but still memorable textual passwords.

Studies of human's memory and emotions, and current password related research are introduced in Section 2. Section 3 explains set-ups of the experiments and the results are presented in Section 4. The usefulness of the study is discussed in Section 5. Section 6 concludes the paper and future work is outlined in Section 7.

2 Related Work

Human's ability to remember is fascinating and lot of research has been done to discover memorizing process and factors that affect it. Several studies have concentrated on how mood, emotional incidence or image of an emotional item affect a person's memory.

Lee and Sternthal studied how mood effect persons learning outcome [19]. The participants were learning names of different brands and the results showed that a positive mood enhanced the learning in relation to a neutral mood.

The study of Dietrich et al. outlined the influence of emotional contents on recognition performance [3]. The set of words were repeatedly presented to a normal subject. If a word was shown for the first time, the participant pushed 'new' button and if the word was already once shown, the participant pushed 'old' button. The words were categorized into three groups: words with positive, negative and neutral content. Positive words were remembered best when controlled 250 ms after stimulus. When control was carried out between 450 ms and 650 ms after stimulus both positive and negative words were remembered better than the neutral ones. The authors concluded that the emotional content had an effect for recognition.

Kensinger et al. examined how emotional content, positive, negative or neutral, affects the amount of remembered visual details [18]. The participants were both young and older adults, and both specific recognition and general recognition were investigated. The results showed that both age groups improved the recognition for the negative objects. Regarding the general recognition, the results were somewhat different. While the older adults showed enhanced recognition for both positive and negative objects, the young adults improved recognition applied only to negative objects.

Psychological studies are not a new addition to password security. For example the findings that images are easier to remember than alphabets, has been adapted to non-textual password schemes such as graphical passwords [6, 14].

In the approach of Gurav et al., the images were used to secure cloud services [6]. Their graphical password consisted of four images. The first two images were selected from an image set, which was selected among nine 100-image sets. The selection was done by an algorithm, which took its seed from the username. The last two images were from the server side. Even though the images are easier to remember than alphabets, several lists of images without any relation to each other are hard to remember. The drawback of this scheme was that it was not scalable as the users with several accounts would have problems to recall the correct password [6].

The graphical password scheme of Jebriel et al. [14] used images drawn by users themselves. The study compared two authentication schemes; a scheme where images were drawn by hand on a paper and afterwards scanned, and a scheme where paint-program was used. The paint-system was preferred because it provided more privacy than the hand-drawing scheme. The privacy was also prioritized over easiness to draw, as the images were more difficult to draw by using a mouse than a hand. Both schemes contained software that corrected drawing errors. The authors suggested that a drawing app where a finger is used for drawing would make the authentication scheme more user-friendly.

Even though the images are easier to remember than textual symbols, the graphical authentication schemes have not been adapted either by the users or the designers. A simple reason is the long transaction time [26]. The security of the graphical authentication schemes is dependent on the amount of the images. The small amount of images means shorter transaction time, but also lower security level. However, Renaud et.al claim the security level can be increased, if the scheme is designed properly [26]. A new scheme, which introduced Captcha as a graphical password, has been proposed by Zhu et al. [29]. This scheme bases on hard AI problems offering both reasonable security and usability.

Despite the graphical password scheme alternatives, the textual password schemes are still mostly used, and the users' behavior regarding to passwords are guided with password policies. Each service using passwords for authentication has a password policy either publicly available or not. AlFayydh et al. investigated several password policies of online services [1]. They found that services having the same authentication assurance level had diverging password requirements. This generates global usability problem. To address this problem they suggested standardized password requirements based on the information security assurance level of the service.

Password guidelines are part of password policies helping the users in their password generation process. The guidelines vary from minimum character set lists to more thorough explanations and examples of password design. Guidelines can be only static or they can be taught either in classroom environment or by e-learning tools. Mwagwabi et al. studied how fear appeals apply to password security and user compliance with password guidelines [21]. Fear appeals consist factors from two main categories: threat appraisal factors and coping appraisal factors. The study showed that perceived threat (degree, which a user worries about password related threats), perceived password effectiveness (degree, which a user believes that recommended password guidelines prevents password threats), and password self-efficiency (a user's confidence to create strong passwords) influence to comply with password guidelines. The study emphasizes that information security training programs should aim to change users' coping appraisal.

3 Experiments

This study consists of two independent experiments conducted in 2012 and 2014. The participants in both experiments were military students who, after finishing the education, are awarded a bachelor degree in engineering and military degree. The experiments took place in a two-week long military exercise, called Exercise

Cyber Endurance. Within these two weeks, students lived in outdoor military bases practicing existing military and engineering skills, and learning new skills. Each day started with physical training called combat conditioning, and at least two simulated military field operations took place. The amount of sleep and nutrition were significantly reduced which meant that the students became more and more tired and hungry, the longer the exercise grew. Access to drinking water was unlimited during the whole exercise period. The participants were 21-27 years old and mostly men. The experiment in 2012 consisted of 34 participants and in 2014 there were 40 participants.

Experiment I

The task in this experiment was to design and recall one traditional password and two sentences; one sentence with a positive content and the other with a negative content. The passwords and sentences were to be a minimum of 13 characters. This setting allowed students to design weak passwords and weak password sentences as there was no requirement for the character sets [8]. The 13 character limit forced students to use at least three words. On the fourth exercise day, the students were asked to design their own individual passwords and sentences. A week after, on the eleventh day of the exercise, the students were asked to write down their passwords.

Experiment II

This experiment was conducted to see if the results of experiment I (with weak password sentences) also applied to a new set of the students and a new test set-up, where strong password sentences were to be remember. This time the students were asked to memorize two 28-character long Norwegian sentences. The positive sentence was 'Sølvi elsker å stå opp kl 6.' (Sølvi loves to get up at 6 o'clock.). The negative sentence was 'Jørn sutrer daglig til kl 9.' (Jørn whines everyday until 9 o'clock.). The sentences included the punctuation marks. Both password sentences are strong passwords [8].

The sentences were given to the students five days before the first recall test, and all students had the same sentences to remember. The sentences were given to students simultaneously. However, the positive sentence was asked first as it was referred to 'start up'-sentence in the larger test set-up and the negative sentence as 'shut down'-sentence.

The larger electronic cognitive test set, also containing the password sentence recall test, lasted ca 40 minutes. The test was conducted three times during the military exercise. The cognitive test set was carried out right after 2x14-minute combat condition training. The first test run was two days before the actual exercise started in the daytime. The second test was on the third day on the exercise (9 days after the students received the sentences) and the third test was on the tenth day on the exercise (16 days after the students received the sentences). The two last tests were conducted between 8 and 11 pm.

Originally, the students were divided into two groups based on the explanations of the tasks in the cognitive test. The first group was a control group. The tasks they conducted were introduced with neutral explanations. In the password sentence recall task, they were only asked to type 'start up' and 'shut-down' sentence. The second group had the same tasks, but now the purpose of each task was explained linking the tasks to cyber security. In the password sentence recall task, they were

Table 1: Recall rates for positive and negative sentence with χ^2-value.

Positive Sentence	Negative Sentence	χ^2
80%	50%	4,267

told that the sentences were passwords and asked to type 'start-up' and 'shut-down' sentences to login-boxes. The second group was called explanation group. The typing procedure was similar to real login procedure, meaning that each character was shown with *-symbol on the login box. The results of other tasks of the cognitive test are to be presented in [11].

4 Results

Results are shown as recall rates. χ^2- test is used due to categorical variables with outcomes *positive content* or *negative content* and *recalled* or *not*. The degree of freedom is one in all comparisons giving the limit for 5% significance level as 3,84.

Experiment I

Two general things were noticed while studying the sentences students had made and tried to recall. When generating the sentences the students often used similar formula for both positive and negative sentences, changing only the verb of the sentence from positive to negative and the object of the sentence. Many of the sentences told which incidences, persons and items students liked and did not like or strongly put, loved and hated. This made the password sentence recalling closer to the task to remember their own favorites and dislikes. All sentences generated in this experiment were weak passwords [8].

For the second, the students were not familiar with the fact that sentences can be used as passwords. When students were asked to write down their passwords, several became lazy to use grammatically correct sentences. They ignored dots, question marks, and exclamation marks that they originally had used. Similarly, some students did not bother to make a difference between upper and lower case letters. However, the actual words were more often correct.

To investigate if the content of a sentence had an effect, the punctuation errors and capitalization errors were therefore ignored, and only correctness of the words was taken into account. The recall rates of positive sentences and negative sentences are shown in Table 1.

The students also made traditional passwords. 66% of these passwords were weak ones and 67% of these weak passwords were recalled correctly. The rest 34% were good or strong passwords. The recall rate for them was 18%.

The χ^2- test indicates that there is relationship between memorability and content of the sentence. In this experiment, the sentences with positive content were remembered better (with 5% significance) than the sentences with negative content.

Experiment II

This password recall experiment was part of the larger cognitive study and therefore the students were divided into two groups based on what kind of introduction to the task they received. The results showed that there were no statistical difference among control and explanation group regarding password sentence tasks. Therefore, we consider all students as a single group and focus on the memorability of the content and the errors students made when typing these password sentences.

The sentences in this experiment were not students' own design. This lowered their overall memorability [30], but kept the analysis simple as the results of the cognitive test needed to be ready immediately after actual test runs. Similarly to Experiment I, it was noticeable that the students were not familiar with the concept 'sentence' as a login secret. The total amount of typed sentences in this study was 235 and in 83% of these, the students did not bother to use punctuation mark. Therefore the punctuation marks were again ignored from the sentences letting the login secrets became 27-characters long. This change lowers the security level of the sentences. The positive sentence stays still strong, but the negative sentence become a good one having a score right under the strong password limit [8].

Similarly to Experiment I, the capitalization errors were also ignored, when analyzing the effect of the content. Both sentences contained the abbreviation 'kl' for the Norwegian word 'o'clock.' The abbreviations are harder to recall than common words because they break normal word processing rules, they are not 'word processing mode', WPM-consistent [15]. As the both 'kl' and 'klokka' or 'klokken' (o'clock) means exactly the same, the students who typed the word instead of the abbreviation did recall the content, but did not recall the right form of it. Memorability of content was only taken into account. Therefore 'klokken' and 'klokka' were accepted.

Table 2 shows the percentages of those passwords where all words and digits were correctly recalled. The table also includes χ^2-values of comparisons between positive and negative sentences. The results show that the positive sentence was better recalled than the sentence with negative content at the first recall test with 5% significance. The differences at second and third test are not statistically large enough to make strong conclusions, and they were also noticed to be slightly biased.

As it can be seen from Table 2, the percentages increase as the exercise moved on. The reason for this most likely lays on the group dynamic. The students were divided into teams during the exercise. Effective teamwork and support from the team members was needed in solving and handling most of the other tasks in the exercise. Even though the cogitative test was individual, we assume that the effect of group work also influences the results of the second and the third test run. The increased rates can be partly explained with the correction of the names used in the sentences. The wrong names in the first test run were corrected to the second or the third test run. There were also cases, where the sentence in first run was totally wrong but halfway or fully correct in the later runs.

In this study, the recall rates are based on memorability of the content ignoring the errors, which in a real login situation would create a login failure. We analyzed these errors and divided them into two categories: typographical errors and missing

Table 2: Percentages of correct sentences

	Pos. Content	Neg. Content	χ^2
1. test (5 d)	58%	30%	6,04
2. test (9 d)	60%	45%	1,81
3. test (16 d)	68%	48%	3,35

detail-errors. Typographical errors in our cases were lack of a single space between words or lack of a letter in a word, a wrong order of the letters in a word and accidental activation of the caps lock. 33% of all typed positive sentences contained some or all these typographical errors. For the negative sentence the typographical error percentage was 40%. The difference is not statistically significant.

The missing detail errors were lack of punctuation mark, usage of a word "klokka" or "klokken" (o'clock) instead of the abbreviation "kl", and lack of spaces between every word in the whole sentence. 82% of the all typed positive sentences and 84% of the all typed negative sentences were missing the punctuation mark. The error in abbreviation was same 26% for both positive and negative sentence. 2% of all typed password were missing all spaces in the sentence.

5 Discussion

In both experiments, the positive sentences were remembered better than the negative sentences and, there were no statistical difference between sentences regarding the typographical error rate and missing detail error rates was found. However, these results cannot be generalized to apply to the whole population and all environments. Our participants were young adults and the tests were conducted in the conditions which were physically hard. Even though, the results presented in this paper support the findings of the other studies and common practices.

Our results are aligned with the findings in the study of Dietrich et al. [3] that showed that the emotional content has an effect for recognition. In their study, positive words were best remembered after very short time (250 ms) and both positive and negative words were better remembered than the neutral ones after a double so long time than in the first case, but still short, time (between 450ms and 650ms) compared to neutral ones.

The positive content is already in use in additional security procedures as they often contain questions about users' favourites. Based on our results, especially from Experiment I, these questions provide answers that are easy for users to recall. However, not everyone has a favorite book or favorite holiday place, and the more user-friendly scheme would be a process where users can select their own 'favourite'-questions.

Keith et al. studied experience and satisfaction of pass-phrases and traditional passwords [16] during a 12-week long experiment period with 56 participants. The participants selected their own pass-phrases with minimum length of 15 characters as well as their own passwords. The average length of the pass-phrases was 19,11 and 7,53 for the control passwords. They did not comment on the contents of the pass-phrases. They found that pass-phases were recalled as well as traditional passwords ($85,86\%$ and $87,5\%$, respectively) when typographical errors were excluded. In general, these percentages are higher than in our study, although they are similar to the recall rate the participants received with their positive pass-phrases in Experiment I.

Keith et al. also found that the pass-phrase users had more failed login attempts due to typographical errors than users with traditional passwords ($19,19\%$ and $2,21\%$, respectively), although these typographical errors disappeared over time [16]. The participants of our study had more typographical errors than the participants in the study of Keith et al.. This might partly be due to the physical exhaustiveness of our students and the fact that the sentences in our study were longer than in the study of Keith et al.

A grammatical correct sentence contains a set of specific items. A sentence always starts with a capital letter. As a minimum, it has a subject and a verb, and each word in the sentence is to be separated from another word with a space. The sentence ends either to a punctuation mark, question mark or exclamation mark. Longer sentences obviously contain more words but they can also easily include for example commas, colons, semi colons, quotes, lines, slashes, parenthesis, and currency symbols. These kind of sentences are 'word processing mode', WPM-consistent. Keith et al. continued their pass-phrase researched in [15]. They found that a pass-phrase should be designed to be WPM-consistent as the users of WPG-consistent pass-phrases had fewer typographical errors than the users whose pass-phrases were not consistent with WPM. In our study, the password sentences were not WPM consistent because of the abbreviation 'kl'. Several typographical errors, such as a lack of a letter, a lack of a space or error in punctuation mark placement, were indeed done around the abbreviation 'kl'.

If sentences are used correctly also in a password setting, the special characters would be included more intuitively than they are included to a traditional password. Sentences belong to Mixture category of the passwords [12], and as long as they contain several words and some digits, they are good passwords. Substitutions, misspellings and mix of different languages make sentences even stronger passwords [13], but also more vulnerable to typographical errors as they are not WPM consistent [15].

The results in this study show that sentences can be used as passwords, but their usage does not seem to be intuitive. The usage of the sentences, which also mean the usage of words, is in contradiction to the guidelines stating that words should not be used. In order to make users' to choose more creative passwords, the users need to be encouraged to update their password designing processes. In practice, this means increasing the amount of updated education.

Password guideline education that bases threat appraisal factors and coping appraisal factors [21] is a good example. Education like that increases users' compliance with password guidelines. Emotional arousal helps humans to maintain a readiness to respond [20]. Examples in education that arouses emotions, influence users perceived threat and perceived password effectiveness. This can be taken further, and by allowing and encouraging users to use sentences as logging secrets, the password policies can help users password self-efficiency.

The use of sentences as passwords might increase the password security among persons with disabilities. Strong traditional passwords; random-looking strings with characters from all character sets, create usability problem for persons with disabilities [9]. Search space entropy of traditional password for persons with Parkinson disease, Dyslexia, upper extremity and visual impairment is lower or slightly lower than for a person with normal capabilities. For persons with Parkinson disease, upper extremity and visual impairment this is due to the difficulties with multiple keys such as uppercase letters and several special characters. For the dyslexics this is due to difficulties to keep characters in the right order, especially in the long words [25]. When the sentences are allowed, dyslexics can create sentences with several short words, which are easier for a dyslexic to type. This will both increase the search space and decrease misspelling errors. For the others, single key symbols such as comma, punctuation mark and space are natural extension for the usable characters when sentences are in use. However, the slower typing speed might make transaction time uncomfortably long and also increase the risk of successful observation attacks.

6 Conclusions

Passwords are used more than ever, but education of password security has not increased neither been updated to meet today's security needs. Today's passwords need to be much longer than eight characters and they should include several special symbols. The long random-looking character strings are very hard to remember, especially when one has to remember tens of passwords. One alternative for the traditional passwords is a sentence containing several words.

This paper includes results of two independent experiments on sentences as login secrets. Both experiments were conducted in a two-week long military field exercise. The participants of the experiments were engineering students of a military school. The goals of the experiments were to learn if a full sentence is usable as a login secret, and if an emotional content of the sentence has an effect to memorability of the sentence.

The results of the experiments show that sentences with a positive content were remembered better than sentences with a negative content. The results also indicate that the long positive sentences is as easily remembered than the shorter traditional password. The typographical error rate and missing details -error rate were similar for both positive and negative sentences.

The length and the special characters like space, punctuation mark, question mark, exclamation mark, comma, colon, semi colon, quote, line, slash, parenthesis, and currency symbols raise the security level of the grammatically correct sentences. Even if the length has a positive effect to security of the sentence, it also has a negative effect to usability of the sentence. The risk of typographical errors increases, when the sentence get longer. However, the typographical errors are not only bound to the length of the sentence, they are also influenced by the writing process [16]. The sentences consisting the elements of the normal writing process with their normal order include less typographical errors than other sentences [16]. Typographical errors also disappear over time [16]. Therefore, it might be wise to practice the typing of the sentence before taking it into use.

The usage of the sentences as a login secret was shown not yet to be intuitive as it is against the password policies that does not allow words to be used. To change the attitudes among users and system designers more updated education is needed.

7 Future Work

The lack of cyber security awareness education [23, 27, 28] does not only concern the adults, but also the children and youth. Several of today's services and entertainments reachable via cyber domain are targeted for children. This means that in order for safe use of these services, the children should know the 'traffic rules' of the cyber domain. However, not all children have this knowledge. Information and cyber security education in Norwegian schools is not mandatory, and the quality of the education varies depending on teacher's own initiative.

To increase the knowledge among school pupils, the Norwegian Centre for ICT in Education launched a project about password education in spring 2014. The purpose of the project is to generate different education packages suitable for pupils in primary schools, secondary schools and high schools. The results of this paper will be useful for these education packages showing the variety of password design possibilities. Hopefully this would then increase the password self-efficiency of the older pupils. For the smallest pupils who are lacking reading and writing skills, different pattern-based 'passwords' are thought to be taught. The goal is to have education packages ready before the school start in fall 2015. We see this project also as an opportunity to change attitudes and update the cyber security awareness.

As discussed earlier, the experiments were conducted during a military exercise with rather small number of participants. Therefore, these experiments can be classified as pilot studies and to confirm the results of these studies, a large follow up study is needed. Experiments can also be used as a part of the education especially when reasons of the current tasks and the findings in the future are explained and discussed with the participants. Therefore, the follow-up experiment can be thought to be carried out among pupils in fall 2015.

References

[1] Bander AlFayyadh, Per Thorsheim, Audun Jøsang, and Henning Klevjer. Improving usability of password management with standardized password policies. In *Proceedings of the 7th Conferance on Networks and Information Systems Security*, 2012.

[2] Sofie Dahlman, Per Bäckström, Gunilla Bohlin, and Örjan Frans. Cognitive abilities of street children: Low-ses bolivian boys with and without experience of living in the street. *Child Neuropsychology: A Journal on Normal and Abnormal Development in Childhood and Adolescence*, 19(5):540–556, 2012.

[3] Detlef E. Dietrich, Christiane Waller, Johannes Sönke, Bernardina M. Wieringa, Hinderk M. Emrich, and Thomas F. Münte. Differential effects of emotional content on event-related potentials in word recognition memory. *Neuropsychobiology*, 43:96–101, 2001.

[4] Abigail Fisher, James M.E. Boyle, James Y. Patron, Phillip Tomporowski, Christine Watson, John H. McColl, and John J. Reilly. Effects of a physical education intervention on cognitive function in young children: randomized controlled pilot study. *BMC Pediatrics*, 11(97), 2011.

[5] Matthew T. Galliot. Hunger and reduced self-control in the laboratory and across the world: Reducing hunger as a self-control panacea. *Psychology (2152-7180)*, 4(1):59–66, 2013.

[6] Shraddha M. Gurav, Leena S. Gawade, Prathamey K. Rane, and Nilesh R. Khochare. Graphical password authentication: Cloud securing scheme. In *Proceedings of the 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies*, pages 479–483, 2014.

[7] Beth M. Hartzler. Fatigue on the flight deck: The consequences of sleep loss and the benefits of napping. *Accident Analysis & Prevention*, 62:309–318, 2013.

[8] Kirsi Helkala. An educational tool for password quality measurements. In *Proceedings of Norwegian Information Security Conference*, pages 69–80, 2008.

[9] Kirsi Helkala. Disabilities and authentication methods: Usability and security. In *Proceedings of the Seventh International Conference on Availability, Reliability and Security (ARES 2012) on FARES Workshop*, pages 327–334, 2012.

[10] Kirsi Helkala and Tone H Bakås. National password security survey: Results. In *In Proceedings of the European Information Security Multi-Conference (EISMC 2013)*, pages 23–33, 2013.

[11] Kirsi Helkala, Silje Knox, and Mass Lund. Changes in cognitive ability during a two-week long military exercise, 2014. To be publized.

[12] Kirsi Helkala and Einar Snekkenes. Password generation and search space reduction. *Journal of Computers*, 4(7):663–669, 2009.

[13] Kirsi Helkala, Nils Kalstad Svendsen, Per Thorsheim, and Anders Wiehe. Cracking associative passwords. In *Proceeding of the 17th Nordic Conference, NordSec*, pages 153–168, 2012.

[14] Salem Jebriel and Ron Poet. Automatic registration of user drawn graphical passwords. In *Proceedings of the 6th International Conference onComputer Science and Information Technology (CSIT)*, pages 172–177, 2014.

[15] Mark Keith, Benjamin Shao, and Paul Steinbart. A behavioral analysis of passphrase design and effectiveness. *Journal of the Association for Information Systems*, 10(2):68–89, 2009.

[16] Mark Keith, Benjamin Shao, and Paul John Steinbart. The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies*, 65(2007):1728, 2007.

[17] Elizabeth A. Kensinger. What we remember (and forget) about positive and negative experiences. `http://www.apa.org/science/about/psa/2011/10/positive-negative.aspx`, 2011. Accesses 3rd June 2014.

[18] Elizabeth A. Kensinger, Garoff-Eaton Rachel J., and Schacter Daniel L. Effects of emotion on memory specificity in young and older adults. *Journal of Gerontology: Phychological sciences*, 62B(4):208–215, 2007.

[19] Angela Y. Lee and Brian Sternthal. The effects of positive mood on memory. *Journal of Consumer Research*, 26(2):115–127, 1999.

[20] Fiona McPherson. The role of emotion in memory. `www.memory-key.com/memory/emotion.`, 2011. Accessed 3rd June 2014.

[21] Florence Mwagwabi, Tanya McGill, and Michael Dixon. Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines. In *Proceedings of the 47th Hawaii International Conference on System Science*, pages 3188–3197, 2014.

[22] Michelon Pascale. Blog. sharpbrains: What are cognitive abilities and skills, and how to boost them? `http://sharpbrains.com/blog/2006/12/18/what-are-cognitive-abilities/`, 2006. Accessed 29th April 2014.

[23] PRWEB. Key findings from security awareness training survey unveiled by security mentor and enterprise management associates. http://www.prweb.com/releases/survey-results-security/awareness-training/prweb4337664.htm, May 2014.

[24] Rainbow tables. https://www.freerainbowtables.com/. Accessed 3rd June 2014.

[25] Stefan Reinhart, Anna-Katharina Schaadt, Michaela Adams, Eva Leonhardt, and Georg Kerkhoff. The frequency and significance of the word length effect in neglect dyslexia. *Neuropsychologia*, 51(7):12731278, 2013.

[26] Karen Renaud, Peter Mayer, Melanie Volkamer, and Joseph Maguire. Are graphical authentication mechanisms as strong as passwords? In *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems*, 837844.

[27] Security Council of Norwegian Industry, NSR. Mørketallsundersøkelse 2012. http://www.nsr-org.no/moerketall/, 2012.

[28] StaySafeOnline. New survey shows U.S. small business owners not concerned about cybersecurity; majority have no policies or contingency plans. http://www.staysafeonline.org/about-us/news/new-survey-shows-us-small-business-owners-not-concerned-about-cybersecurity. Accessed 3rd of June 2014.

[29] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu. Captcha as graphical passwordsa new security primitive based on hard ai problems. *IEEE Transaction on Information Forensics and Security*, 9(6):891–904, 2014.

[30] W.J. Zviran, M.and Haga. A comparison of password techniques for multilevel authentication mechanisms. *Computer Journal*, 36(3):227–237, 1993.