Writing down your password: Does it help?

Vanessa Boothroyd
Carleton University
Ottawa, Canada
Email: vanessa.boothroyd@gmail.com

Sonia Chiasson
Carleton University
Ottawa, Canada
Email: chiasson@scs.carleton.ca

***Abstract*—Users are able to remember their phone numbers and postal codes, their student numbers, PIN numbers, and social insurance numbers. Why, then, do users have trouble remembering their passwords? This paper considers the hypothesis that being able to access written notes when needed would eventually help users to memorize the password. Further we hypothesize that writing down passwords encourages the use of passwords that are more complex than their unwritten (memorized) counterparts. We surveyed 31 participants on their opinions and experiences with writing down passwords and tested whether these participants created more complex passwords when they were encouraged to write them down. Finally, we observed whether written passwords had higher login success rates when tested again at least one week later. Results indicate that regardless of the experimental condition, users preferred to memorize their passwords than to take the extra step of referring to their written notes. Additionally, memorized and written passwords were remembered equally well. Finally, we found that users who had difficulty logging in had passwords with significantly higher mean entropy, which confirms the heuristic that complex passwords are harder to remember. We also unexpectedly found that users password habits are so strongly ingrained that they often ignored our instructions about writing or memorizing their password and continued to use their preestablished strategy. This observation is noteworthy for anyone conducting user authentication research.**

I. Introduction

Passwords remain the most common form of user authentication available online. However, the problems with passwords are well known [1], [2]. Users often choose insecure, memorable passwords that are vulnerable to password guessing attacks. The secure alternative of assigning random passwords suffers from significant usability problems since most users are unable to effectively memorize several random strings of alphanumeric and symbol characters.

Besides selecting weak passwords, users also resort to other coping mechanisms, such as writing down their passwords. In this paper, we explored the effectiveness of this coping strategy. We address two research questions: *Does writing down passwords help users remember them?* and *Does it encourage the creation of more complex passwords?* We conducted a week-long user study with 31 participants to investigate these two issues.

Our results were unexpected. Encouraging users to write down passwords did not result in stronger passwords, nor did it help them to remember them at a later date. We did find that those users had login failures were using passwords that had significantly higher mean entropy than those users who logged in successfully every time. We also uncovered some methodological issues that may serve as a warning to other usable security researchers. Some of our participants had password behaviors that were so ingrained that they failed to comply with their encouraged study condition. Without careful post-study evaluations, results of the study would have been unknowingly skewed.

The remainder of the paper is organized as follows. In Section II, we discuss current password behaviors and common password advice. Section III includes our hypotheses and describes the study methodology. Section IV presents our detailed data analysis. Sections V and VII discuss the insights gained from the study and conclude the paper.

II. Background

Most users must interact with authentication systems on a daily basis and most of these systems require users to employ a previously memorized textual password. Research indicates that users typically create simple passwords and frequently reuse these passwords across different accounts [1]–[3]. This reduces the cognitive load of creating and remembering a growing number of passwords, but also results in the ”Password Problem”. The Password problem describes this situation where users choose easy-to-remember passwords to deal with the increasing number of accounts they must manage, but these passwords are also easy for attackers to guess. Password reuse further compounds the problem because attackers who break into one account may be able to gain access to the user's other accounts protected by the same or similar passwords.

Password managers offer another alternative to managing multiple passwords, but these have their own issues that render them unsuitable in some situations. They have been shown to suffer from usability problems that result in weaker security than if users managed their passwords themselves and some users are reluctant to trust all of their credentials to a third-party [4]. They also result in a single point of failure; if an attacker breaches the password manager then all of the user's accounts are potentially compromised.

Assuming that users are going to manage their own passwords, plenty of advice instructing users how to create stronger passwords currently exists. The advice typically includes using a seemingly random combination of uppercase and lowercase letters, digits, and symbols, but these are difficult for users to remember [5]. If forced to comply with these rules, users may resort to further coping strategies to offload the burden. For example, they may write down their passwords [1], [6], [7], although some do so "apologetically" [8] because they believe it is insecure. Security experts have mixed opinions of whether writing down passwords is a reasonable strategy. Several researchers argue that writing down passwords compromises security [1], [6], [8]. However, Schneier [9] recommends writing down passwords and keeping them in a safe place. There are two potential problems with this behaviour. The password could be found by someone and used maliciously; this will not reduce security against outside attackers, but shifts the threat from an unknown online attacker to someone in the physical proximity of the user. The other risk is that the written password could be lost, in which case the user would need to go through the system's password recovery steps. In this study, we explore the potential benefits of writing down passwords while taking these drawbacks into account. Keep in mind that without access to a person's username, having a user's password is of little use.

III. Study Design

We explored the common coping mechanism of writing down passwords so that users do not need to worry about remembering them because they may be referenced when needed. Specifically, we investigated the experiences, opinions, practices, and outcomes of writing down passwords.

We formed the following two hypotheses:

Hypothesis 1: Users who are encouraged to write down their password will formulate more secure passwords than those users advised against writing down their password.

Hypothesis 2: Users who wrote down their password will have more successful logins than those users who did not write down their password.

Our first hypothesis was based on the assumption that users who were encouraged to write down their password when creating an account would create passwords that were more complex than those of other users. The rational behind this hypothesis is that users who know prior to password creation that they may write down their password would not have to worry about creating a memorable password because they could reference the written password at any time. Users in the memory condition would need to create a password that they could remember for future logins, without the luxury of referring back to a written copy. Our second hypothesis stemmed from the idea that the user with written passwords could refer to them as needed and so would have higher login success rates than those who simply memorized them.

The act of writing down a password and being able to reference it when necessary may help with memorization, as this is how users often memorize other strings of characters such as a postal code or a credit card number. We suggest that after using their written password a number of times, the user will have memorized it, and will therefore no longer need to reference the written cue. They would no longer need to keep the password in an accessible place and may destroy the written evidence, or may choose to place the notes in a more secure location such as a locked filing cabinet. This practice may be considered a more secure way to manage text based passwords.

A. Participants

Thirty-one participants between 21 and 37 years of age were recruited via targetted convenience sampling from two university campuses, a seniors' centre and the community at large. Participants had varied educational backgrounds. Every participant self-assessed their computer skill level to be moderate or higher, and accessed the internet at least several times a week (94% accessed it daily). Participants were each renumerated ten dollars after having completed the final stage of the study.

B. Protocol

We conducted a three-part study which involved an initial in-lab session with the experimenter and two home based sessions. The study used the MVP authentication testing framework [10] and a custom blog called World Vacations; a website about vacation destinations created at Carleton University for the purposes of authentication studies. The web-based system was instrumented to record relevant authentication information such as usernames, passwords, login attempts and password resets. Each time a participant logged in to the website to leave a comment, we were able to see the entered password, as well as keep track of how many times the passwords were successfully used, erroneously input, or reset.

The study used a between-subjects design in which participants were randomly assigned to either the *Written* condition or the *Memory* condition. Prior to their password creation, participants in the *Written* condition were encouraged to write down their passwords "so you won't forget" them. At the time of password creation, users were provided with pen and paper to do so. In the *Memory* condition, participants were asked to not write down their passwords "to keep everything secure", and were not provided with pen and paper.

Initial lab session: Participants met individually with the researcher and the initial lab session was run as follows:

1) Users were provided with a username and received instructions on whether they should write down their password or not
2) Users created a password for the World Vacation website
3) Users confirmed their password by entering it again
4) Users completed a short demographics questionnaire
5) Users answered a pre-test questionnaire regarding their opinions and attitudes towards writing down passwords
6) Users logged in to the World Vacation website and posted a comment

Users were encouraged to create a password that was as secure as possible, and asked not to re-use an existing password because we would be able to see the system logs. Passwords were required to be between 6-10 characters in length, but no other restrictions were imposed.

Online follow-ups: Participants received e-mail twice over the following week, asking them to log in to their blog account and comment on a blog post. This was done to test password memorability. Consistent with earlier work on password memorability [6] , the emails were sent on Day 3 and Day 7 after password creation. According to Florencio and Herley [2], this roughly reflects the frequency with which users log in to many of their real accounts. Lastly, participants were asked to complete a final online survey about their experiences and practices of writing down passwords.

IV. Analysis and Results

Our analysis includes statistical comparison of login successes and password resets between conditions, frequency evaluation of questionnaire responses, and qualitative analysis of open-ended questions and user comments.

A. Pre-Test results: Current password habits and perceptions

At the start of the session, users completed a pre-test survey to gather their current experiences and opinions regarding writing down passwords and password reuse. The pre-test questionnaire included the seven questions listed below.

1) Have you been told not to write down passwords? (Yes/No)
2) Have you been told writing down passwords decreases security? (Yes/No)
3) How do you think writing down your password affects the safety of your accounts? (open-ended)
4) Do you sometimes re-use the same password on different web sites? (Yes/No)
5) Does having a password written down allow you to better remember it after you use it a few times? (Yes/No)
6) Would you be more inclined to choose a more secure (complex) password if you were able to write it down and refer to it later? (Yes/No/Maybe)
7) Would you be as inclined to use the same password for many different accounts if you were able to write them down and refer to them later? (Yes/No/Maybe)

In the remainder of this section, we group results thematically for simpler discussion. We use three main themes reflecting previous advice received by users, personal beliefs about writing down passwords, and possible behaviour change resulting from permission to write down passwords.

Previous advice: Most users had received advice regarding writing down passwords. We found that 70% of users had previously been told not to write down their passwords and 63% of users had been told that writing down passwords decreases security. These results demonstrate the prevalence of the idea that writing down passwords reduces security and that people should not write down their passwords. Whether this advice is sound remains to be seen.

Personal beliefs about written passwords: When asked for their personal opinion on writing down passwords, users voiced security and usability concerns. We coded these open-ended responses and aggregated similar responses. Data coding involves identifying keywords or ideas in participant responses (themes). Results are summarized in Figure 1.

We found that 48% of users felt that the safety of a written password depended on where the password is stored. Some users worried about others having "physical access" to the written passwords and explained how that risk could be mitigated by storing it in a "safe" location. For example, storing it in a notebook at home was considered safe while posting it on a computer at work was considered unsafe. Ten percent of users considered that writing down passwords has no impact on security, and one person mentioned they never write down passwords, but instead write down clues as to what the password might be. Others had strategies for keeping electronic records safe such as using a password manager or including it in an email to themselves.

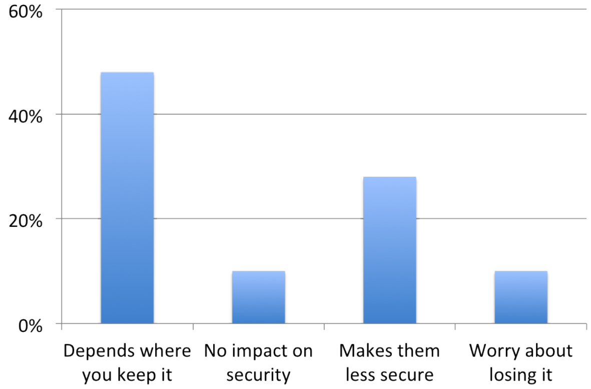

Fig. 1. Perception of how writing down a password impacts its security

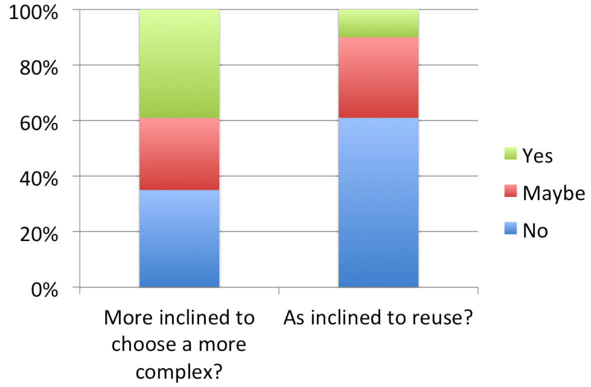

Fig. 2. User attitudes if written passwords were permitted

Twenty-eight percent of users felt that writing and storing passwords is always less secure than simply memorizing them. They were concerned about the risk of having a written password stolen or accidentally discovered by someone. Ten percent of users also worried about losing a written password and being unable to access the associated account (or having to resort to using the website's password reset service). Participants also reported using other coping behaviors with respect to passwords. For example, 97% of users admit to reusing passwords.

Permitting written passwords: Many users felt that there were (or would be) benefits if writing down passwords was permitted. Half of users felt that writing down passwords would improve memorability of the passwords at a later date. Six of the 31 users commented that the act of writing down or typing a password offers opportunity to practice it and helps them to remember the password.

As summarized in Figure 2, 39% of users stated that they would be more inclined to choose more complex passwords if they could write them down. In explaining their responses, a further 6% reported that they already write down their password so that a hypothetical situation in which this was permitted would not change their behaviour. At the opposite extreme, 13% claimed they already used complex passwords, so writing them down would make no difference.

However, 61% claimed that they would be less likely to reuse passwords if writing them down was allowed. Of the remaining participants, a further 29% were unsure if they would reuse. When asked to explain their responses, 19% said they would reuse passwords only for trivial or unimportant account if allowed to write down their passwords. A small group of users remained wary of writing down passwords even if it was allowed. We found that 13% of participants disliked the idea of having to refer back to the written password and 7% were too worried about losing the written password.

Summary of pre-test results: Most users have been told not to write down their passwords and that writing down passwords decreases their security. Despite this advice most users recognize that the security of a written password is highly dependent on how that password is stored. Most users saw utility in writing down passwords and many currently write down at least some of their passwords. Many users felt that if writing down passwords was permitted and encouraged, they would create stronger passwords and be less inclined to reuse passwords.

B. "Adoptive" conditions

During testing our participants were assigned to either the *Written* condition or the *Memory* condition. At the end of the study, we asked participants whether they had actually complied with their respective conditions and found that a few participants had done the opposite of what they were encouraged to do. Six participants in the *Written* condition said that they had simply memorized their password without writing it down and three participants in the *Memory* condition revealed that they had written down their password. For the analysis, we moved these participants to their respective "adoptive" conditions. The remainder of the analysis includes twelve participants in the *Written* condition and nineteen participants in the *Memory* condition.

Since several participants "adopted" different conditions, the sample size for the *Written* condition is smaller than expected and this likely impacted the statistical significance of the results. In several instances, the data suggests differences but these are not statistically significant with this sample. This may demonstrate how ingrained users' password management practices are, and may speak to challenges regarding experimental validity for future password studies which attempt to control how users manage their passwords.

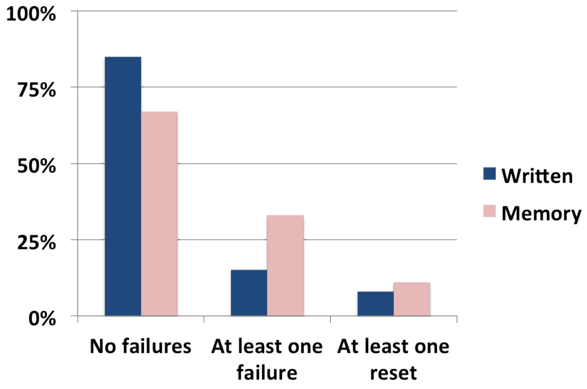

Fig. 3. Login Failure Rate per Condition

C. Login Successes, Failures and Resets

We examined login success rates after users final login to the World Vacations website. The data includes any login attempt made after Day 6. Every user was eventually successful at logging in to the World Vacation website and commenting on the blog from their home as part of the later sessions. Some users did make errors and some needed to reset their password. Figure 3 summarizes the login and failure results.

A failure is recorded when a user submits a password that is incorrect and access to the blog is denied. Results show that 33% of users in the *Memory* condition and 15% of users in the *Written* condition had failures; the remainder were able to log in successfully on the first attempt. However, chi-square tests completed on these failure rates indicate the number of users who failed did not differ significantly by condition. We report the number of users who had a password failure rather than the number of total failures to indicate the proportion of users who experienced difficulty. The number of failures can be skewed by personality traits and preferences; for example, one user may fail once and decide to reset their password, while another may re-try a dozen times, which confounds the results.

A password reset involves the user inputting an incorrect password, and upon receiving the notification that the password was incorrect, opting to create and confirm a new password rather than trying to input their password again. Every reset also counted as a failed login since users only had the option of resetting after a failure. Eleven percent of users from the *Memory* condition and 8% from the *Written* condition reset their passwords.

Overall, users in both conditions coped fairly well with remembering their password. From Figure 3, it appears that those in the *Memory* condition had more difficulty, but these results were not statistically significant.

D. Password entropy

The NIST password entropy calculation [11], as described in NIST Special Publication 800-63, was used to calculate

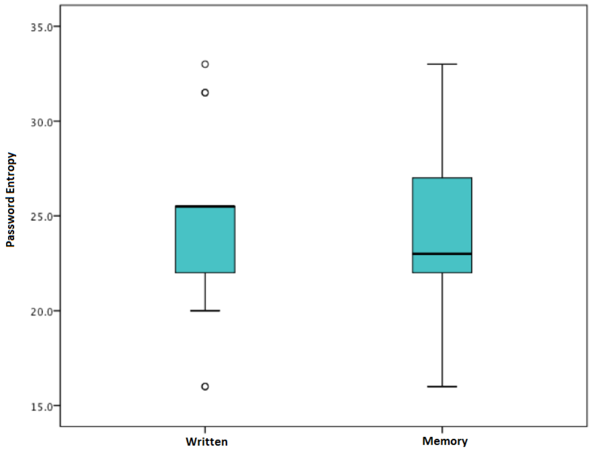

Fig. 4. Mean password entropy in bits.

password entropy. The calculation assigns scores to individual passwords based on characteristics such as the number of uppercase characters, password length, a dictionary check and the inclusion of non-alphabetic characters.

Contrary to our expectations, password entropy did not differ significantly between groups. Those users in the *Written* (adoptive) condition created passwords with a mean entropy of 24.5 bits and a standard deviation of 5.4. Those users in the (adoptive) *Memory* condition created passwords with a mean entropy of 23.9 bits and standard deviation of 5.1. A summary of the results are shown in Figure 4. An independent samples t-test shows no statistically significant differences between the two groups.

Interestingly, while there were no differences between conditions, we found that users with stronger passwords were more likely to have failed login attempts. post-hoc analyses found that those passwords that were used in failed login attempts had significantly higher entropy (M = 27.6, SD = 4.4) than those passwords that did not fail (M = 23, SE = 4.9); $t(29) = -2.4, p < .05$.

While the NIST entropy calculation offers a rough approximation of password strength, it cannot account for all features that may strengthen or weaken a password. We further explored users' choice through visual inspection of the passwords. As expected, we found that many passwords followed conventional patterns such as being related to the website/task, combining words and numbers, or containing a simple number sequence. However, we found that 30% of *Written* passwords followed no simple or obvious pattern while only 15% of *Memory* condition passwords appeared random based on our inspection. This would need further exploration with a larger dataset, but it provides weak support for the hypothesis that writing down passwords encourages stronger password choices.

E. Post-study questionnaire

At the end of the week-long study, participants completed a questionnaire regarding their choice of password and the perceived strength of that password. Our intention was to assess whether users who could write down their passwords believed they were selecting stronger passwords (even if they had misguided beliefs about what constitutes a strong password).

The four Likert-scale questions are listed below and Figures 5 to 8 illustrate users' responses. We discuss results for each question separately.

1) I chose a password that was particularly memorable to me.
2) My password would be easy for attackers to guess.
3) My passwords are unlikely to have any meaning to other people.
4) I think other people would choose the same passwords as I did.

I chose a password that was particularly memorable to me: As summarized in Figure 5, 39% of users in the *Memory* condition strongly agreed that they had chosen a particularly memorable password while only 11% strongly disagreed. Only 23% of users in the *Written* condition indicated that they strongly agreed with the statement and 23% strongly disagreed. While not statistically significant, these findings are still interesting with the differences likely due to the participant's condition. Users who wrote their password down may have worried less about remembering their password, which likely affected their password choice. There was no correlation between a users' opinion of choosing a password that was particularly memorable to them and their passwords' NIST estimated entropy.

My password would be easy for attackers to guess: 33% of users in the *Memory* condition strongly disagreed that their password would be easy for an attacker to guess. Users in the *Written* condition responded similarly, with 31% strongly disagreeing. Responses are summarized in Figure 6. While it is unsurprising that most users would consider their password hard for an attacker to guess, it is interesting to note that there is no significant correlation between how respondents answered this question, and the NIST entropy of their passwords. Users may interpret password "guessability" or strength differently than those who defined the NIST password entropy estimate guidelines.

My passwords are unlikely to have any meaning to other people: Thirty-five percent of users in both the *Written* and *Memory* conditions indicated that they strongly agreed that their passwords were unlikely to have meaning to other people (see Figure 7). 70-80% of users answered 5 or above (agree to strongly agree) to this question. Again, there is no correlation between their passwords' NIST entropy and whether they thought their password would have meaning to other people. Interestingly, the majority of users seems to consider their password to be private and/or somehow random, regardless of whether their password actually is strong in practice.

I think other people would choose the same passwords as me: Similarly, users believed that their passwords were somehow unique to them. As seen in Figure 8, more than

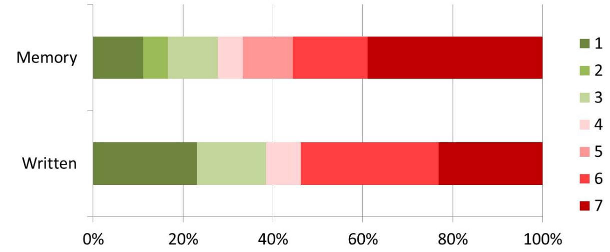

Fig. 5. Responses to "I chose a password that was particularly memorable to me." (1 = strongly disagree, 7 = strongly agree

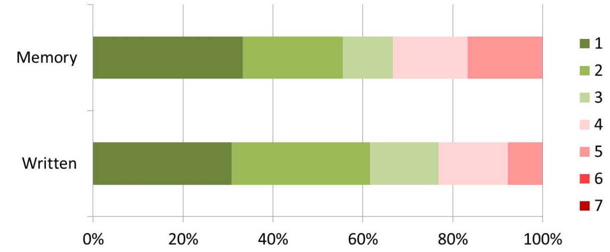

Fig. 6. Responses to "My password would be easy for attackers to guess." (1 = strongly disagree, 7 = strongly agree

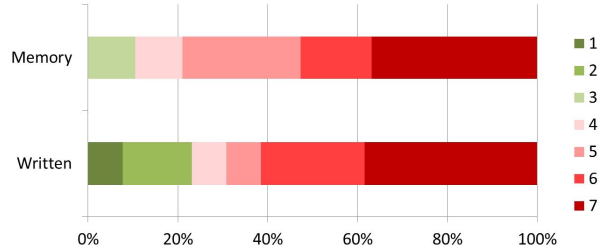

Fig. 7. Responses to "My passwords are unlikely to have any meaning to other people." (1 = strongly disagree, 7 = strongly agree

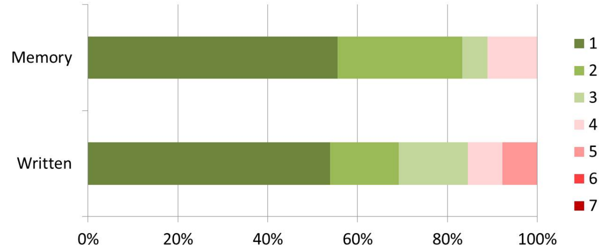

Fig. 8. Responses to "I think other people would choose the same passwords as me." (1 = strongly disagree, 7 = strongly agree

half of users in both conditions strongly disagreed with the statement that others would choose similar passwords.

Post-hoc analyses: Post-hoc analyses demonstrated a significant positive correlation between the question about others choosing the same passwords (Question 4) and whether users thought their password would be easy for attackers to guess (Question 2), $r(29) = 0.47, p < .01$, indicating that users understood the relationship between these two concepts. Further, as should be expected, a significant negative correlation was found between users' responses to whether they thought other people would choose the same password (Question 4) and whether their password would have meaning to others (Question 3), $r(29) = -0.4, p < .05$. These significant correlations demonstrate consistency in participant responding.

Overall these Likert-scale responses indicate that users felt that they chose secure passwords. They thought that their passwords would be difficult to guess, that the passwords were unlikely to have meaning to other people, and that other people would be unlikely to choose similar passwords. Approximately two thirds of users answered positively to choosing passwords that were memorable. Interestingly, users clearly believe that they are effectively balancing memorability and security, even though our empirical results suggest otherwise.

F. Support for hypotheses

Returning to our two initial hypotheses, we found little support in this study for either hypothesis.

Hypothesis 1: Users who are encouraged to write down their password will formulate more secure passwords than those users advised against writing down their password.

Based on the NIST entropy calculations, this hypothesis was not supported by our data. However, visual inspection of the passwords suggests that those who wrote down their passwords were in fact more likely to choose "random" looking passwords.

While the experimental condition had no impact on the measured strength of passwords, users in both conditions similarly *perceived* their password as difficult for attackers to guess, unlikely to be meaningful to others, and unlikely to be similar to other people's passwords.

Hypothesis 2: Users who wrote down their password will have more successful logins than those users who did not write down their password.

We found no support for this hypothesis. There was no significant difference between the adoptive *Written* condition and the adoptive *Memory* condition. More users in the *Memory* condition had password failures than those in the *Written* condition, but not to a significant degree.

Our post-hoc analysis showed that regardless of condition, users with stronger passwords according to the NIST estimates had more difficulty logging in after one week.

V. Discussion

Up to this point we have described results from each of the different perception measures, performance measures and entropy measures separately. In this section we discuss what these results may mean when taken together. The results of our study were unexpected and we reflect on the interpretation of the results and on lessons learned from the study.

Switching Conditions/Methodology Users have strong opinions regarding password management and seem to have already decided on a password strategy to manage their own accounts. The resulting password management behaviours become password management habits, which our users seemed reluctant to break. A number of users maintained their habitual password management strategy during the study, despite having initially been encouraged to adopt different one. While users were specifically encouraged to follow their assigned strategy, it is possible that some users interpreted the instructions as simply one option/suggestion and decided to follow their own strategy because it was most familiar. We discovered this behaviour during post-study analysis and unfortunately could not return to ask users why it occurred.

This non-compliance makes it difficult to evaluate differences between study conditions. Future studies regarding user behaviour may necessitate larger numbers of participants to mitigate the effects of non-compliance. Alternatively, a different study design could let users behave as they would normally rather than try to assign them to specific conditions. This design would reflect more realistic behaviour, but makes it difficult to assess novel strategies since no users have adopted them yet.

Complex passwords are difficult to remember: Our post-hoc analysis showed that users who had difficulty logging in had significantly higher password entropy than those who had no login failures. While unsurprising, this supports the assumption that higher entropy passwords containing symbols, numbers, and uppercase, and lowercase letters are indeed harder to remember.

In related work, Komanduri et al. [6]) advise that “a 16-character minimum with no additional requirements provides the most entropy while proving more usable on many measures than the strongest alternative”. Our results suggest that this advice may be effective. However, many authentication systems do not support this type of password. We suggest that system administrators reconsider minimum password requirements to improve password entropy and usability without mandating numbers, symbols, and upper and lower case letters.

Users’ perceived password strength is misguided: Our users believed that they were creating strong passwords, but this did not often translate into strong passwords according to the NIST guidelines. This may indicate that users do not understand how password guessing attacks work. Explaining to users how password attacks work rather than simply telling them to use symbols and/or numbers in their passwords may be more effective in terms of changing user behaviour and inciting them to use different or better passwords. Although not an ideal strategy, education on what constitutes a strong password is still necessary. Ideally, users should not be tasked with managing passwords, but they will realistically need to do so for the foreseeable future. While this is the case, we should endeavor to enable users to make informed decisions.

Contradiction between prevalent advice and user attitudes: Despite having been advised not to write down passwords, many users recognize that writing down a password is not an insecure behaviour in itself, but that the risk lies in the storage/handling of the password once it is written. We propose that rather than warning users against writing passwords (which is advice that is often ignored anyway), the security community should consider how to best advise those who insist on writing down passwords. For example, advising users to create different, complex passwords, and to store them in a secure location. Other useful advice may be to write down clues as to what the password might be rather than writing the password itself, to mitigate against anyone who finds the written clues being able to gain access to the account in question. Further, keeping the usernames for various accounts in a separate location from the passwords may also be valuable security advice for users.

These strategies will not work for everyone. We also found a significant number of users who refused to write down their password because of the inconvenience of retrieving the written note or because of fear of misplacing the written note. Advice should instead focus on helping users best secure their existing strategies rather than encouraging completely different management methods.

VI. Study Limitations

As a small lab study, some limitations should be considered while interpreting the results. Our users were primarily young, university-educated users. While this represents a large number of frequent internet users, it may not generalize to the entire population. Secondly, users created passwords for an account on a travel location blog. Users may not have felt this type of account was particularly important to protect or that a password was not protecting anything of value. However, ethical considerations in password research make it difficult to ask users to divulge passwords for accounts that protect real personal or private information, therefore a balance must be achieved between ecological validity and ethical concerns. In this case, we were more interested in relative password entropy between the two conditions and users’ perceptions of the strength of their password rather than absolute password strength, so opted for the current methodological approach.

Future Research Future research should explore the effects of education on users’ accuracy in estimating their password’s entropy and their password creation strategies.

VII. Conclusion

We investigated the effects of encouraging users to write down their passwords. We hypothesized that those who could write down their password would perform better and create stronger passwords than those who were simply memorizing their password. However, our results did not support these hypotheses. Instead, we found that users’ password habits are ingrained and users are reluctant to modify their behaviour, even when instructed to do so. Writing down passwords did not significantly improve password memorability or password entropy. Further, users overestimate the security of their own passwords. These results have significant implications for how we should educate users about password security and for how user studies of password behaviours are designed.

ACKNOWLEDGMENTS

The authors thank Elizabeth Stobert for her guidance and assistance with the study design and using the MVP password management system. Sonia Chiasson holds a Canada Research Chair in Human Oriented Computer Security and acknowledge the Natural Sciences and Engineering Research Council of Canada (NSERC) for funding the Chair and a Discovery Grant. Both authors acknowledge funding from NSERC ISSNet.

REFERENCES

[1] A. Adams and M. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, December 1999.

[2] D. Florencio and C. Herley, "A large-scale study of web password habits," in *WWW '07: Int. Conf. on World Wide Web*. ACM, 2007.

[3] S. Gaw and E. Felten, "Password management strategies for online accounts," in *SOUPS: Symp. on Usable Privacy and Security*. ACM, 2006.

[4] S. Chiasson, P. C. van Oorschot, and R. Biddle, "A usability study and critique of two password managers," in *USENIX Security Symposium*, 2006.

[5] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *Security & Privacy, IEEE*, vol. 2, no. 5, pp. 25–31, 2004.

[6] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of Passwords and People: Measuring the Effect of Password-Composition Policies," in *Proceedings of the 29th Conference on Human Factors in Computing Systems (CHI)*. New York, USA: ACM, 2011.

[7] B. Grawemeyer and H. Johnson, "Using and managing multiple passwords: A week to a view." *Interacting with Computers*, vol. 23(3), pp. pp. 256–267, 2011.

[8] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *SIGCHI Conference on Human Factors in Computing Systems, (CHI)*. ACM, 2010.

[9] B. Schneier. (2005, June) Write Down Your Password. In 'Schneier on Security'. [Online]. Available: http://www.schneier.com/blog/archives/2005/06/write_down_your.html

[10] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. Freitas Machado, A. Forget, N. Wright, G. Chan, and R. Biddle, "The MVP Web-based Authentication Framework," in *Financial Cryptography*, 2012.

[11] W. E. Burr, D. F. Dodson, and W. T. Polk, "NIST Special Publication 800-63: Electronic Authentication Guideline," NIST: US National Institute of Standards and Technology, Gaithersburg, USA, Tech. Rep., 2006.