MWAIS 2018 Proceedings

Midwest (MWAIS)

5-2018

# Password Memorability and Strength using an Image

Cameron Burns
*Missouri University of Science & Technology*, cbfmb@mst.edu

Nathan Twyman
*Missouri University of Science & Technology*, nathantwyman@mst.edu

# Password Memorability and Strength using an Image

**Cameron Burns**
Missouri University of Science & Technology
cbfmb@mst.edu

**Nathan Twyman**
Missouri University of Science & Technology
nathantwyman@mst.edu

## ABSTRACT

In this study, the goal was to determine if the use of an image may help the average user to create strong and unique passwords, as well as give aid to remember the password that was created. Furthermore, we aim to determine if the image helps improve the perception of security. The way we went about this was to develop a survey that provides the user with an image and asks them to create a password that may be strong enough for a school account using that image. Four groups were tested, a control with no image and three test groups each featuring a unique image.

### Keywords

Passwords, Memorability, Memory, Password Strength, Images, Password Helpers, Perception

## INTRODUCTION

As computers become more advanced and processors grow ever faster, it becomes easier for them to crack passwords that were once deemed secure. As users, it is important that we combat this any way we can in order to keep our data safe. The ability to create a strong, secure password is more important than ever; however, having a strong password is meaningless if it is too difficult to remember. Memorability is the challenge because if a password is too complex then users may resort to techniques that could leave them more at risk. Writing passwords down, repeating them across various services, or using the "set and forget" mentality, where they count on remaking their password each time they wish to access the service, are all such practices.

The goal of this study was to test a new method that may be used in some form to help users create stronger passwords and more importantly give them something with which to associate the password so they may better remember it. A study done by students at Carleton University states, "Some users may also more easily remember their passwords if they can visualise them" (Forget, Chiasson and Biddle, 2008). In that study it appears they were actually visualizing the passwords in the sense that characters would be around the screen in a pattern and it was the pattern that revealed the password. With this in mind it was decided that utilizing pictures may be an effective method, so three images were found and utilized for the experiment. Several images were used to insure there wasn't some bias on that specific image and that the method would work on images in general. They were intentionally colorful and busy so users would likely be drawn to different parts of each image, which should result in more unique passwords. Each of the images not only featured different objects but also a different general color palette, focal point, and sizes of objects within them. This was done to determine if the significant differences between the images and their individual traits made a meaningful impact in relation to the password that the user would create and its effectiveness on their memorability.

Ideally we strive to find that the use of an image would assist users in not only the creation of complex and effective passwords, but to remember them as well. Specifically for accounts that may require a more secure password such for schools, businesses, and other areas of interest that would require a solid line of defense. The use of such images for the creation such strong passwords will significantly reduce the rising threats that are emerging in this evolving technological age. Given this, as stated prior beforehand, the best way to keep one's personal digital data secure is with a complex, yet memorable password which can be possibly resolved through this method.

## METHODOLOGY

Subjects were randomly divided into one of four groups, where they were asked to create a password using standard rules, such as the use of mixed-case alphanumeric characters and symbols as well as a length of at least ten characters. Ten characters was the chosen length because it is slightly longer than the average, which is, according to an analysis done on the leaked Sony account passwords, somewhere between six and eight characters (Hunt, 2011). This being the higher end of the spectrum would likely mean there would be less variation in strength based on length alone as users may struggle to get there and would be less likely to make passwords much longer. Ten characters would also probably be more difficult to remember than a password of a standard length, which is important as the goal was to determine if users would remember more complex passwords. Only length was enforced, with the rest being at the discretion of the user, so they would have the final say as to how strong their password would be after the required length. The password field was not hidden so the password they created was available for them to see as they typed in plain text. The test groups were each provided with one of three images and asked to create a password using the image. The control group was not provided with an image but was given the same rules and asked all the same questions except questions that directly pertain to the image used for the control groups.

In an attempt to lead subjects away from focusing on the password they were asked to create, the survey was disguised as a test of grammar. The belief was this would serve as a good distraction as it put other words at the forefront of their thoughts. To further push the idea that it was a test about grammar and that the password was only to secure their results, subjects were also asked if English was their primary language. The grammar portion consisted of fifteen questions divided up to five questions per page across three pages to reduce survey fatigue.

Upon completion of the grammar portion of the survey the subjects are presented with the image that they used, if they had one. Users were then asked to input the password they created, this time in a password field where the typed text was hidden by black dots. The response was accepted whether or not the password matched the one used at the beginning so it could be tested if the user was actually able to remember their password or not. Following the input of the password, questions relating to the user perception are asked. These questions were specifically whether they believed the presence of an image helped them to recall the password. Furthermore, they were asked of how unique and memorable they felt the password was

Qualtrics was utilized for the development of the survey and the survey was distributed to students of Missouri University of Science and Technology of varying majors and seniority. This accounted for roughly a third of participants. The remainder of subjects came from Amazon's Mechanical Turk and 4Chan's Worksafe Requests board. The demographics otherwise are unknown.

## DATA ANALYSIS

When the survey was administered the goal was to obtain at least 30 participants within each of the four groups for a total of 120 people. The number 30 was determined as any significant difference across groups would be able to be seen with such a sample size. After distribution, 137 people in total completed the survey. Of the four groups 31 were placed in the control, 28 were assigned to IMG1, 34 were assigned to IMG2 and the final 39 were placed in the group with IMG3. The average length across all groups was 13 characters for the passwords created which helped to prevent from any wild changes in strength based on length alone. The average time it took a user to complete the entirety of the survey was six minutes and fifteen seconds.

Given that each group had a required length of 10 characters most of the passwords were classified as strong by a lot of password strength checker websites. I opted to utilize rumkin.com to test password strength by bits listed by entropy (Atkins, 2017). This means it is tested by the amount of bits as well as how common characters were when placed adjacent to other characters and how long it would take for someone to crack the password. The website determines this by using letter pair combinations in the English language. Strength in bits was the primary test however the percent of passwords that were correctly input as well as perceived security were also tested.

The data displayed below is mostly intact with the only real adjustments being to remove outliers determined by bit strength. Some data was also removed where it was obvious the user did not utilize the image at all by using passwords such as "password", "abc123", as well as "9876543210". Since the objective was to determine if the an image increased memorability or security responses like this did not prove or disprove anything related to the experiment. That being said there were other questionable data points that were left in because they were unique passwords where it was unable to be determined if the image was used. At the end of the experiment after outliers and irrelevant data had been removed, 30 remained in control, 28 with IMG1, 24 with IMG2 and 31 remained in the group with IMG3

Another important thing to note is during the survey the second time subjects entered their password they were not able to see the password they used and were not corrected if the password wasn't a match. Some errors appeared here as Qualtrics does not warn users if Caps Lock is active. An outlier was removed from the control as it had 90 characters and a bit strength of 465.2 and another from IMG3 group as it had 82 characters and a bit strength of 424.6. Both of these super-inflated the average strength of the group they were in.

| GROUP | Average Strength<br>(in bits) | Percent Correct | Perceived Memorability<br>(7-point Scale) | Perceived Strength<br>(7-Point Scale) |
|---|---|---|---|---|
| Control | 54.61290 | 81.25% | 5.59 | 5.18 |
| IMG1 | 63.19166 | 79.91% | 5.25 | 5.79 |
| IMG2 | 63.86071 | 75.00% | 5.14 | 5.23 |
| IMG3 | 59.11379 | 82.75% | 4.48 | 4.93 |

**Table 1. Survey Data**

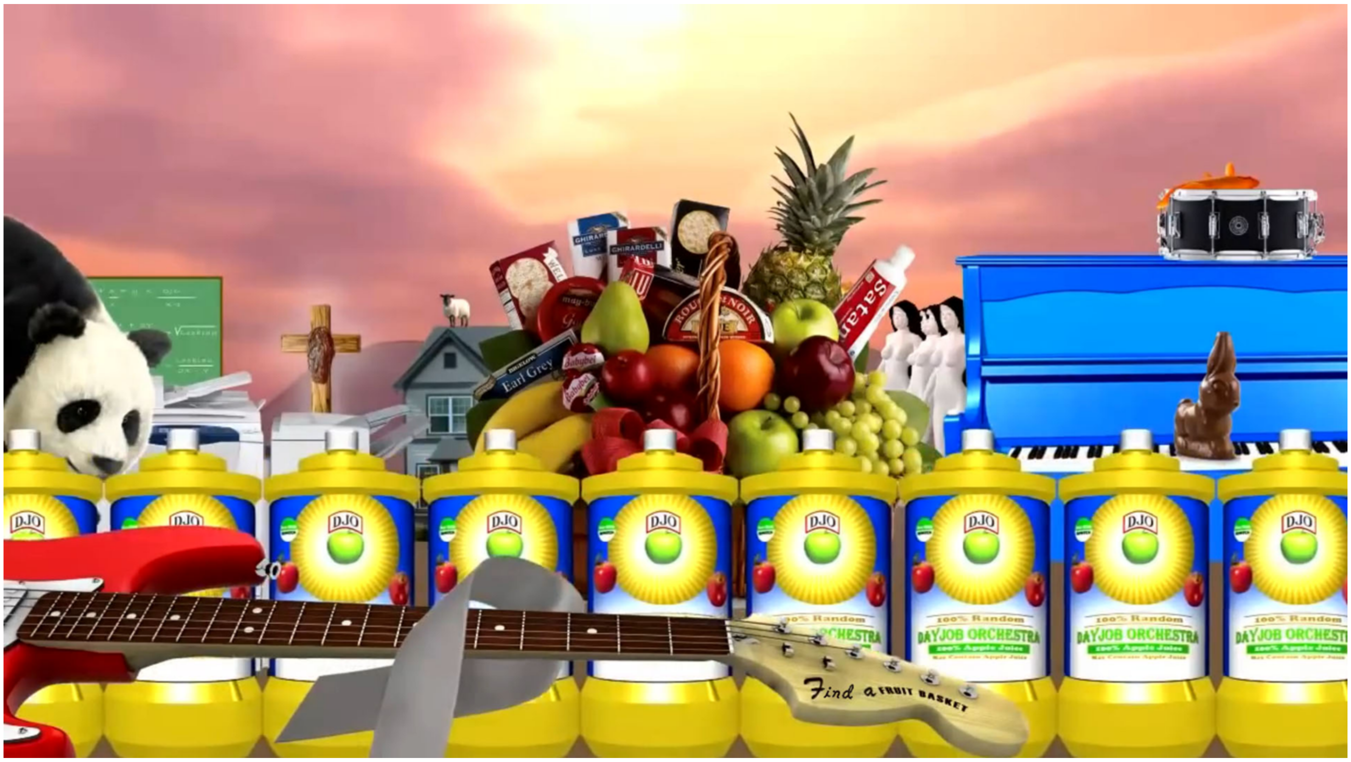

**Figure 1. IMG1**

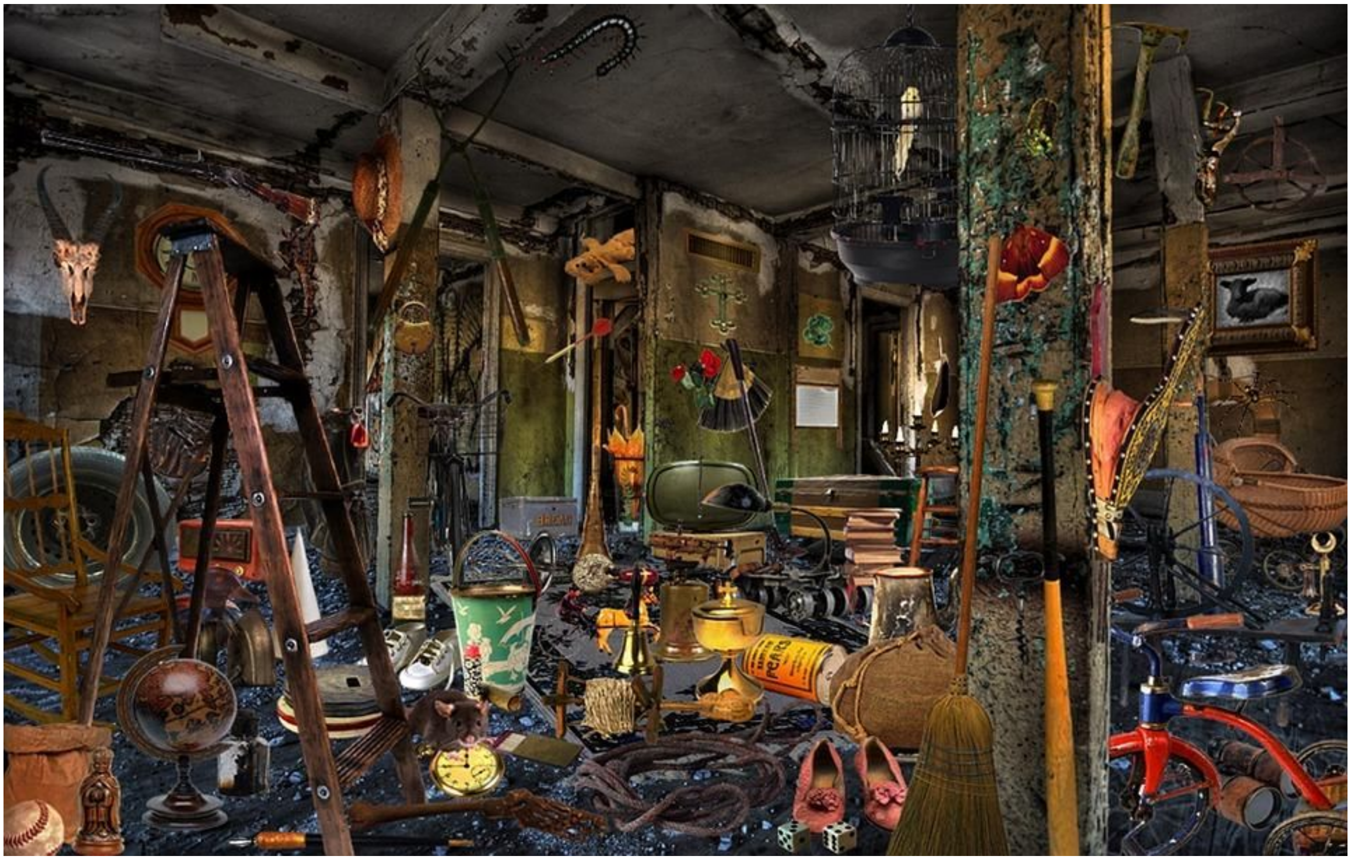

**Figure 2. IMG2**

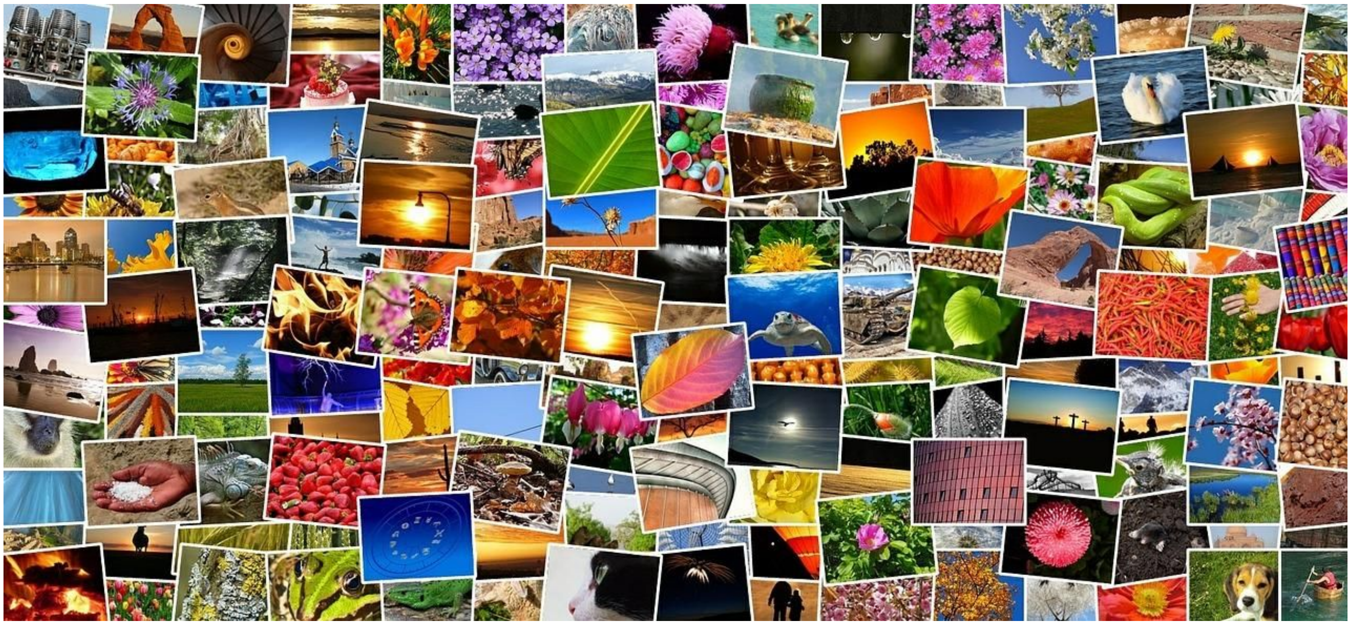

**Figure 3. IMG3**

## DISCUSSION

Overall, it appears as though the use of an image did help to increase strength as the average bit strength of each group provided with an image was higher than the group that did not have an image. However, the use of a picture did not increase user perception of password memorability. The three images each had a different response on the perception of strength for reasons that are unclear. IMG1 allowed for users to create a much higher strength than the control as well as a higher perceived strength.

It is important to note that there are issues with using a helper to remember passwords. Using an image, it may be easy to come up with a dictionary attack after analyzing the graphic, song or whatever may be used to identify a password. That is a limitation of this method, that may be solved by someone down the line but is not the focus of this experiment. It may help this issue by having a huge library of images. That way it wouldn't be feasible to build a dictionary of words that would likely encompass all the images. This however may lead to other issues such as storing the images used or how to call them for each unique user. If each username were associated with an image then they may be put at a greater risk because an attacker could simply get a hold of the username to display the image and build a dictionary around that user's image. This would certainly make it harder to crack passwords en masse however it doesn't necessarily help the individual. Once again there are limitations that may be brought about by the use of this method on a large scale.

Currently this method could be used by an individual if they chose. It would be reasonable to keep an image in their wallet or on their smartphone. A picture in either place wouldn't seem out of place and certainly wouldn't mean anything to a bystander unless they were told that the image was a hint for a password. The data does show that this method increases the strength of a password and while it may not conclude that an image is definitively better for assisting in the memorization of the password it also does not prove that an image damages the memory of the password.

Future studies may want to add a focus on the specific images to determine if a type of image may be better at generating complex, memorable passwords, such as a collage compared to a hidden object image. There are many factors that would need to be analyzed such as number, type, size and color of objects. Larger objects and brighter colors may draw more attention and thus cause more users and as a result more passwords to home in on that part of the picture. What helps a user to identify a strong password is another aspect that should be looked into for future studies, especially since the data shows that the passwords are in fact stronger, it would be important to find out why users do not believe as such.

## CONCLUSION

Overall, we have determined that the use of an image can be used to create more complex and effective passwords; however, it currently lacks in the  substantial effect on memorability. The data collected from this experiment supports this as the passwords created with the image from the test were more complex than those from the control group. It is plausible to say, however, that through future research the use of an image can be practically employed as to create both memorable and potent passwords. As technology evolves it is evident that individuals will need more complex and efficient ways to protect their information, and this method may potentially become both an effective countermeasure to our growing online security problem.

## REFERENCES

1. Atkins, Tyler. “Strength Test.” Strength Test, rumkin.com/tools/password/passchk.php, accessed November 16, 2017
2. Forget, A., Chiasson, S., and Biddle, R. (2008) Lessons from Brain Age on Password Memorability, *Proceedings of the 2008 Conference on Future Play, Share, 262-263.*
3. Hunt, Troy (2011) “A brief Sony password analysis”, Troy Hunt, troyhunt.com/brief-sony-password-analysis, accessed October 5, 2017