Empowering Users: Leveraging Interface Cues to Enhance Password Security

Yasmeen Abdrabou[1,2], Marco Asbeck[3], Ken Pfeuffer[4], Yomna Abdelrahman[2,5], Mariam Hassib[2,6], and Florian Alt[2]

[1] Lancaster University, United Kingdom
[2] University of the Bundeswehr Munich, Germany
[3] LMU Munich, Germany
[4] Aarhus University, Denmark
[5] European Universities in Egypt
[6] fortiss Research Institute of the Free State of Bavaria, Munich, Germany
y.abdrabou@lancaster.ac.uk

Abstract. Passwords are a popular means of authentication for online accounts, but users struggle to compose and remember numerous passwords, resorting to insecure coping strategies. Prior research on graphical authentication schemes showed that modifying the interface can encourage more secure passwords. In this study ($N = 59$), we explored the use of implicit (website background and advertisements) and explicit (word suggestions) cues to influence password composition. We found that 60.59% of passwords were influenced by the interface cues. Our work discusses how designers can use these findings to improve authentication interfaces for better password security.

Keywords: Passwords · Authentication, · User Interface · Usability.

1 Introduction

Up to date, passwords remain the most popular means for authentication [10]. Although different authentication techniques such as behavioral biometrics or facial recognition, it is unlikely that password usage will be eliminated anytime soon [3]. This is due to the advantage of passwords over other techniques such as ease of use, and security [4]. As a result, people have on average 80 accounts they are protecting with an average of 3.5 passwords. This makes password memorability challenging [7].

Numerous methods have been developed to help users obtain stronger passwords. Besides explicit approaches, such as password policies which may force users to create secure passwords, there are also promising implicit attempts to steer the user in a certain direction. Von Zezschwitz et al. [18] presented an interesting approach, where they showed that by carefully choosing a background image to the Android lock pattern, they were able to significantly reduce the use of popular start positions.

In this work, we adopt this approach for text-based passwords. In a remote study, we explore the concept of integrating explicit (i.e word suggestions to be added to the password) and implicit (i.e. UI elements, advertisements, background images) UI cues on password composition.We found that 60.59% of composed passwords were influenced by the interface cues. To our knowledge, this is the first study exploring the effect of UI cues on password composition.

2 Related Work

The trade-off between usability and security has been the subject of continuous research in both academia and industry. Security experts consider users to be the weaker link in the security of systems because they lack the motivation to create secure passwords. The enormous number of accounts per user (80 on average) [7] makes password memorability challenging. Hence, users create mitigation techniques, such as reusing passwords [13].

To address these problems, researchers have proposed different approaches. Yan et al. [17] suggested using mnemonic phrase-based passwords, integrated into the generated passwords. The results showed that this approach is as secure as random passwords and more secure than regularly chosen passwords. Furthermore, Jermyn et al. [8] suggested altering the order of the chosen password after creating it. Other schemes explored include fictional news headlines [9], word associations [11] or use passphrases [12]. Seitz et al. [14] suggested using the *Decoy Effect* to influence password composition. The authors developed concepts to improve persuasive approaches to nudge users towards stronger password creation. Recent works suggest adding gaze as a behavioral aspect to increase password strength and reduce reuse [2, 1].

Another body of research investigates influencing users' password composition. For example, research showed that adding a background image to the authentication screen guided participants to create stronger and lock patterns. For example, Dunphy et al. [5] showed that adding a background picture to the "Draw A Secret"graphical password approach significantly increased the complexity of the drawn passwords. A similar study by Von Zezschwit et al. [18] showed that users choose patterns based on their interest in the geometric properties of the resulting shapes. Hence, the authors implemented an approach to nudge users to create more diverse passwords by adding or animating a background image. Furthermore, Ur et al. [15] implemented a password meter that provides accurate strength measurement and actionable, detailed feedback to users to help them modify their created passwords.

Finally, one work that explored altering text-passwords generation is the research by Forget et al. [6]. They introduced *Persuasive Text Passwords (PTP)*, a text password system that leverages Persuasive Technology principles to influence users to create more secure passwords. After users choose a password during creation, the PTP system improves the password's security by placing randomly-chosen characters at random positions into the password. Users can shuffle the order and position of the randomly-chosen characters until they find

a memorable combination. Results showed that the PTP variations significantly improved the security of users' passwords.

Motivated by prior research, in this paper, we will investigate using implicit (i.e., background images) and explicit (i.e., word suggestion) UI cues to influence users' text-password choice on different websites with different protected information sensitivity.

3 User Interface Cues and Password Composition

In this section, we will reflect on the study design and the design choices. This research covers one research question **RQ**, *What are the implications of adding implicit/explicit UI cues on text-password composition?*

3.1 Study Design

To address our research question, we conducted a within-subjects study with remote participants who completed all conditions. Our study had two independent variables: 1) implicit and 2) explicit UI cues, and 1) high and 2) low sensitivity of website information. The dependent variable was the generated passwords. Our study was GDPR compliant, with participants able to opt-out at any time, and their data being deleted. We obtained consent from participants to analyze and share their collected passwords. Moreover, we collected participants' eye gaze data on the website to map where did they look during the study. Finally, we collected a post-study questionnaire that asked participants to reflect on their collected passwords and provide Likert scale responses on how frequently they use PayPal and 9GAG (ranging from 1 "rarely" to 5 "daily").

3.2 User Interface Design and Cues

To investigate the impact of interface cues on password creation, we utilized two different types of cues: 1) implicit and 2) explicit cues. Implicit cues were added to the interface to inspire participants to incorporate them into their passwords, including a background image, advertiser logo, dynamic content, ticking counter for PayPal, and GIFs for 9GAG. Explicit cues suggested a phrase or password that users could use partially or fully to create their passwords. The plain registration webpage included only the website logo, and after 2 seconds, a fading sentence suggesting a word to make the password more personalized appeared. Users could select two categories of interest from 15 presented at the beginning of the study, such as education, literature, gaming, and others. We used two different websites to assess the influence of data sensitivity levels: PayPal, with high-sensitivity information such as users' full name, address, gender, and bank details, and 9GAG, with almost no personal user information saved. Both websites included three fields to enter: email, password, and password reentry. Our design was based on the original website designs to collect ecologically valid data, with a password strength meter included to encourage participants to create stronger passwords. Figure 1 shows the different interface designs.

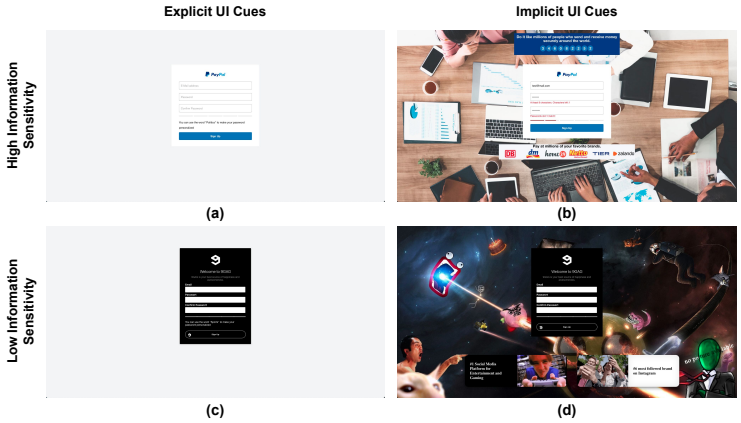

Fig. 1. A screenshot of our implemented two websites with their two variations. (a) and (b) represent high information sensitivity webpages, and (c) and (d) represent low information sensitivity webpages.

3.3 Apparatus and Participants

As our study was remote, we implemented a JavaScript and Node.js website for the study. We used MongoDB Atlas for the database, we hosted it on Heruku and we use GazeRecorder for eye tracking[7]. We also disabled auto-completion for passwords to make sure that participants created the passwords and did not use password meter suggestions.

We recruited 59 participants (30 Females and 29 Males), aged 18 to 54 ($M = 24.67; SD = 5.83$). Participants had diverse nationalities and backgrounds, including, Engineering, law, secretaries, and workers. Participants had different nationalities from USA, Germany, Italy, UK, Turkey, India, and Russia. 12 participants had glasses on, and 7 had corrected vision using lenses. Participants did not have IT security background or experience ($M = 1.5$ on a scale from 1 (novice) to 5 (expert))), and finally, most of our participants use PayPal frequently (71.19%); however, they do not use 9GAG frequently (89.83%).

3.4 Procedure

We recruited participants via university mailing lists and directed them to a study URL. After reading the study's aim and consenting to data collection and analysis, they were directed to an eye-tracking calibration page. Participants were asked to register and sign in on two different websites with two variations, shown in counterbalanced order. Participants were informed that the interfaces are only replicas of the original websites. Afterwards, they filled a demographics

[7] https://gazerecorder.com/gazecloudapi/

form. The study lasted 15 minutes and participants received 5 Euros as compensation. As this was a deception study, we debriefed participants with the main aim of the study in the end, and they were allowed to opt-out.

3.5 Limitations

Our study was able to overcome some of the limitations of remote studies by collecting ecologically valid data, while also being able to maintain a high level of participant engagement, as evidenced by the lack of reported interruptions. Furthermore, our study showed promising results in terms of short-term password memorability. To build on these findings, future research could explore the long-term effects of using cues to enhance password memorability.

4 Evaluation Methodology

To decide if the interface inspires the passwords, we defined key aspects that would indicate that the password is inspired by the implicit cues such as:

1. Website name or adapted website name (replacing letters with numbers or special characters) (i.e PayPal30EusikR)
2. Background item names (i.e Zalando5432)
3. Items description (Name, Color, Size, Position, etc) (i.e bigEyesCat9)

For the explicit cues, we indicate that the explicit cue inspires the password if the password contained the cue itself (i.e. Sports5432), or a subtopic of the cue (i.e p!zZa123 when primed with the category. If a password, for example, contained the website name (implicit cue) and the explicit cue, then we consider the longest (in terms of the number of characters) of them, and we use its respective category for counting.

We used a two-step approach for both categories: First, we used an automated process to compare collected passwords to a predefined set of words (e.g., PayPal, pizza, blue). Second, we manually checked the remaining passwords for letter replacements with numbers or special characters (e.g., p!zza, P@yPal).

5 Results

5.1 Passwords Overview

In total, we gathered 236 passwords from participants who agreed to share them, with an average length of 11.5 characters. Table 1 presents a selection of passwords collected for each cue type (implicit and explicit) and website content sensitivity level (high and low). Before analyzing the passwords, we needed to verify that participants had not simply entered random characters. To achieve this, we employed the zxcvbn password meter [16] to evaluate password strength. Our analysis revealed that the average password strength score was 2.43 out of

4 (on a scale from 0 (easily guessable) to 4 (hard to guess)), indicating that participants created passwords that were not easily guessable.

To assess the memorability of the passwords, we asked participants to log in to the websites at the end of the study. Our results showed that 86% of the logins were successful, which suggests that the passwords were reasonably memorable.

Table 1. Sample of the passwords collected per cue type (Implicit and Explicit) and per website content sensitivity (High and Low)

	Implicit Cues (Background)	**Explicit Cues (Word Suggestion)**
High Information Sensitivity (PayPal)	dbToLate247	TravelSriLanka94
	Paypa!123	MoviesCollection1999!
	Zalando5432	1234Petsarecute
	Netto123123	Fashion@Style.1998
	banking4518	spo3rtsisFun
Low Information Sensitivty (9GAG)	ExploringMemes	CocaColaisGreat
	alienCakememe	Footballer94!
	pokemonfstgen	Studytechnology1
	bigEyesCat9	9GAG4FUNtechnology
	9gagsonde3851	Timis1niceActor

5.2 Password Characteristics Per Webpage Content Sensitivity

Looking at the password strength relative to the content sensitivity, we found that high-sensitivity information (PayPal) is slightly stronger (average strength score of 2.59 (on a scale from 0 (very week) to 4 (very strong))) than low-sensitivity webpage (9GAG) 2.34. A repeated-measures ANOVA with Bonferroni correction showed that the content sensitivity significantly affects the created password strength ($F_{2,118} = 4.44$, $P = .037$). We also found that the length of the passwords created for PayPal and 9GAG 11.89 and 11.10 characters, respectively, is another indication of our participants' website sensitivity perception, which confirms the literature [1]. However, stronger passwords can also mean less memorability. Evidence of this is provided by the login success rate, which is 82% for PayPal compared to 89% for 9gag.

5.3 Password Characteristics Per UI Cue Type

Implicit cues resulted in slightly stronger passwords (avg. strength score of 2.52) compared to explicit cues (2.41), but this difference was not statistically significant according to a repeated measures ANOVA. Passwords affected by explicit cues were slightly longer than passwords inspired by implicit cues (11.63 vs. 11.36 characters), but the cue type did not have a statistically significant effect on password length. Passwords affected by implicit cues had a higher successful login rate (92%) compared to ones affected by explicit cues (80%).

5.4 Cues Impact on Passwords Generation

Of the 236 passwords collected in our study, 60.59% (143 passwords) were influenced by the interface cues. Of these, 44.76% (64 passwords) were influenced by implicit cues (i.e. background) and 55.24% (79 passwords) by explicit cues (i.e. word suggestion). Our statistical analysis, using repeated measures ANOVA with Bonferroni correction, showed that the type of cue significantly influenced the generated password ($F_{1,118} = 83.904$, $P < .001$). Users' gaze heatmaps on the different interfaces also reflected this finding, as seen in Figure 2.

Participants created stronger passwords when using interface cues (score of 2.86 on a scale from 0 to 4) compared to not using any cues (score of 2.18), as shown in Figure 3. Interface cues significantly influenced the strength of passwords (ANOVA $F_{1,59} = 19.98$, $P < .001$). Successful login attempts were associated with passwords inspired by interface cues in 60.89% (123 out of 202) of cases, compared to 39.11% (79 out of 202) of attempts with passwords not influenced by interface cues.

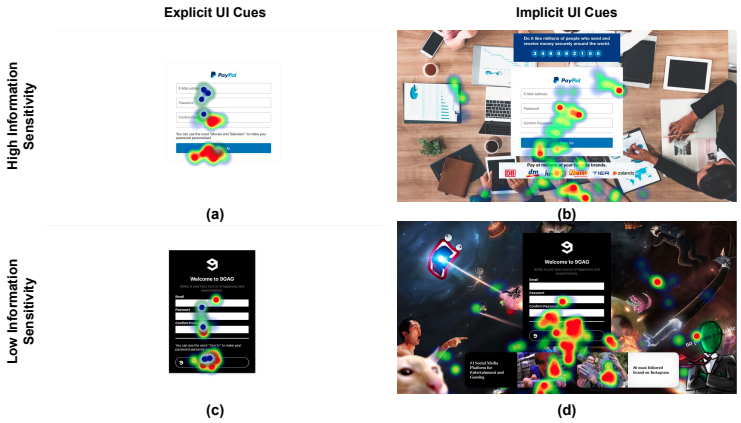

Fig. 2. Eye gaze heatmaps for the four interfaces highlighting P2 gaze data. The heatmaps show that for implicit cues, users looked at background objects that they later used in their passwords. Similarly, for the explicit cues, users who looked at the word suggestion were inspired by it.

For the *High Sensitivity Webpage (PayPal)*, we found that 59.32% (35 out of 59 passwords) of the passwords generated were influenced by the implicit cues, and 79.66% (47 out of 59 passwords) were influenced by the explicit cues. This is slightly higher than the percentages for the *Low Sensitivity Webpage (9GAG)* where we found that 49.15% (29 out of 59 passwords) of the passwords were inspired by the implicit cues and 61.10% (36 out of 59 passwords) were inspired by the explicit cue, comparison can be seen in Figure 4. However, for both implicit and explicit cues, we could not find a statistically significant effect

of the interface cues on the passwords generated according to each information sensitivity level ANOVA test, $P > .05$.

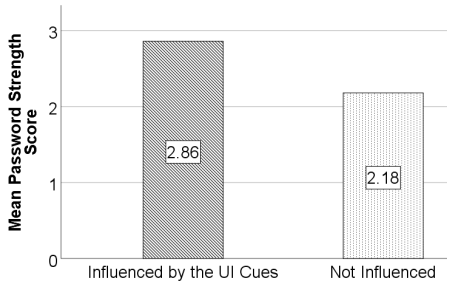

Fig. 3. Mean password strength score for passwords influenced and not influenced by the UI cues.

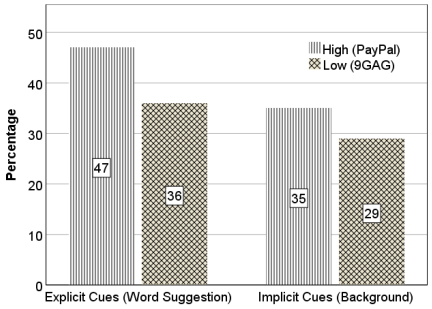

Fig. 4. Percentage of passwords influenced by a) Implicit & b) Explicit cues added to registration webpages with information sensitivity levels a) High and b)Low.

6 Discussion

The results of this study have several implications for the design of website registration pages and the use of UI cues to impact users' password composition. Our findings suggest that incorporating UI cues into the registration process can have a positive impact on the strength and memorability of passwords. This is an important contribution to the field, as it demonstrates how UI cues can influence password composition and highlights the potential benefits of incorporating such cues into the design of registration pages.

In particular, our study found that UI cues increased the strength of passwords created by users compared to passwords not influenced by the cues. This is a significant finding, as it suggests that UI cues can be an effective tool for improving the security of user-generated passwords. Additionally, we observed that having UI cues enhanced the memorability of passwords, as reflected in the proportion of successful login attempts. While our preliminary findings are promising, a longer-term study is needed to test the lasting effect of UI cues on password memorability.

Another interesting finding from our study is that passwords influenced by implicit cues were stronger than those influenced by explicit cues, although the difference was not statistically significant. One possible explanation for this result is that explicit cues limit users to the word suggestion, whereas implicit cues provide a broader range of suggestions. This highlights the potential benefits of providing implicit cues throughout the registration process to encourage users to generate stronger and more memorable passwords.

However, it is important to note that there may be potential security risks associated with the use of UI cues in password composition. Specifically, if users become too reliant on UI cues to generate passwords, they may be more vulnerable to various types of attacks. Moreover, UI designers could potentially manipulate users to choose a certain type of password, which raises ethical concerns. Further research is needed to investigate these potential threats and to ensure that cue-based text passwords are sufficiently secure.

Despite these concerns, our findings suggest that incorporating personalized UI cues into website registration pages can be an effective tool for improving the security and memorability of passwords. These cues can be learned from users' behavior or entered by the user in advance into the system. Our approach can also leverage personality traits and adaptive user interfaces to create UI cues accordingly. We envision that our approach can be integrated into internet browsers to add personalized content to websites or can be used by designers to create adaptive, personalized registration pages. Overall, our study offers valuable insights into the potential benefits and limitations of UI cues for improving password composition and highlights avenues for future research in this area.

7 Conclusion & Future Work

In this study, we aimed to investigate the impact of using implicit (e.g. website background and advertisements) and explicit (e.g. word suggestions) cues on password composition. To achieve this, we conducted a remote user study and collected passwords from 59 participants. Our analysis revealed that 60.59% of the generated passwords were influenced by the UI cues. Additionally, we found that the use of UI cues led to stronger passwords compared to those not influenced by the cues. However, it would be valuable to conduct a follow-up study to investigate password memorability over longer periods and explore alternative representations of UI cues that can implicitly impact password choice.

References

1. Abdrabou, Y., Schütte, J., Shams, A., Pfeuffer, K., Buschek, D., Khamis, M., Alt, F.: " your eyes tell you have used this password before": Identifying password reuse from gaze and keystroke dynamics (2022)
2. Abdrabou, Y., Shams, A., Mantawy, M.O., Ahmad Khan, A., Khamis, M., Alt, F., Abdelrahman, Y.: GazeMeter: Exploring the Usage of Gaze Behaviour to Enhance Password Assessments. Association for Computing Machinery, New York, NY, USA (2021), https://doi.org/10.1145/3448017.3457384
3. Alt, F., Schneegass, S.: Beyond passwords—challenges and opportunities of future authentication. IEEE Security & Privacy (2021), http://www.florian-alt.org/unibw/wp-content/publications/alt2021ieeesp.pdf, alt2021ieeesp
4. Bonneau, J., Herley, C., van Oorschot, P.C., Stajano, F.: Passwords and the evolution of imperfect authentication. Commun. ACM **58**(7), 78–87 (jun 2015). https://doi.org/10.1145/2699390, https://doi.org/10.1145/2699390

5. Dunphy, P., Yan, J.: Do background images improve draw a secret graphical passwords? In: Proceedings of the 14th ACM conference on Computer and communications security. pp. 36–47. ACM (2007)
6. Forget, A., Chiasson, S., Van Oorschot, P.C., Biddle, R.: Improving text passwords through persuasion. In: Proceedings of the 4th symposium on Usable privacy and security. pp. 1–12. ACM (2008)
7. Hanamsagar, A., Woo, S.S., Kanich, C., Mirkovic, J.: Leveraging Semantic Transformation to Investigate Password Habits and Their Causes, p. 1–12. Association for Computing Machinery, New York, NY, USA (2018), https://doi.org/10.1145/3173574.3174144
8. Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.: The design and analysis of graphical passwords. In: 8th USENIX Security Symposium (USENIX Security 99). USENIX Association, Washington, D.C. (Aug 1999), https://www.usenix.org/conference/8th-usenix-security-symposium/design-and-analysis-graphical-passwords
9. Jeyaraman, S., Topkara, U.: Have the cake and eat it too - infusing usability into text-password based authentication systems. 21st Annual Computer Security Applications Conference (ACSAC'05) pp. 10 pp.–482 (2005)
10. Komanduri, S., Shay, R., Kelley, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F., Egelman, S.: Of passwords and people: Measuring the effect of password-composition policies. Association for Computing Machinery, New York, NY, USA (2011). https://doi.org/10.1145/1978942.1979321, https://doi.org/10.1145/1978942.1979321
11. Pond, R., Podd, J., Bunnell, J., Henderson, R.: Word association computer passwords: The effect of formulation techniques on recall and guessing rates. Comput. Secur. **19**(7), 645–656 (nov 2000). https://doi.org/10.1016/S0167-4048(00)07023-1, https://doi.org/10.1016/S0167-4048(00)07023-1
12. Porter, S.N.: A password extension for improved human factors. Computers & Security **1**(1), 54–56 (1982)
13. Seitz, T., Hartmann, M., Pfab, J., Souque, S.: Do differences in password policies prevent password reuse? In: Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems. p. 2056–2063. CHI EA '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3027063.3053100, https://doi.org/10.1145/3027063.3053100
14. Seitz, T., von Zezschwitz, E., Meitner, S., Hussmann, H.: Influencing self-selected passwords through suggestions and the decoy effect. In: Proceedings of the 1st European Workshop on Usable Security. Internet Society, Darmstadt. vol. 2, pp. 1–2 (2016)
15. Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., Cranor, L.F., Dixon, H., Emami Naeini, P., Habib, H., et al.: Design and evaluation of a data-driven password meter. In: Proceedings of the 2017 chi conference on human factors in computing systems. pp. 3775–3786 (2017)
16. Wheeler, D.L.: zxcvbn: Low-Budget password strength estimation. In: 25th USENIX Security Symposium (USENIX Security 16). pp. 157–173. USENIX Association, Austin, TX (Aug 2016), https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler
17. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password memorability and security: empirical results. IEEE Security Privacy **2**(5), 25–31 (2004). https://doi.org/10.1109/MSP.2004.81

18. von Zezschwitz, E., Eiband, M., Buschek, D., Oberhuber, S., De Luca, A., Alt, F., Hussmann, H.: On quantifying the effective password space of grid-based unlock gestures. In: Proceedings of the 15th International Conference on Mobile and Ubiquitous Multimedia. pp. 201–212. ACM (2016)