Exploring the Acceptability of Graphical Passwords for People with Dyslexia

Polina Evtimova and James Nicholson

Northumbria University, Newcastle, UK
james.nicholson@northumbria.ac.uk

Abstract. Alphanumeric passwords are still the most common form of user authentication despite well-known usability issues. These issues, including weak composition and poor memorability, have been well-established across different user groups, yet users with dyslexia have not been studied despite making up approximately 10% of the population. In this paper, we focus on understanding the user authentication experiences of people with dyslexia (PwD) in order to better understanding their attitudes towards a graphical password system that may provide a more inclusive experience. Through interactive interviews, participants were encouraged to try three different knowledge-based authentication systems (PIN, password, and graphical password) and then discuss their strategies behind code composition. We found that PwD employed potentially dangerous workarounds when composing passwords, in particular an over-reliance on pattern-based composition. We report on how PwD do not immediately see the benefits of graphical passwords, but upon experiencing the mechanism we see opportunities for more inclusive authentication.

Keywords: Dyslexia, authentication, passwords, graphical passwords, HCI.

1 Introduction

Alphanumeric passwords are the most common form of digital authentication and best practice dictates that these should not be reused in order to prevent opportunistic attacks (e.g., credential stuffing). The danger of reusing passwords has become more salient to everyday users recently due to sustained data breaches and the regular publication of large breach compilation on popular hacking forums. In particular, the publication of 3.2 billion individual records, including cleartext passwords, on February 2021 [1] serves as a clear example of the suboptimal nature of user passwords.

However, there are well-known cognitive and social factors [2] that act as disincentives for users to conform to gold standard password advice. Despite recent government advice shifting towards usable recommendations, e.g. the National Cyber Security Centre in the UK advocating for length over complexity [3], password management continues to be problematic for many users [4].

People with dyslexia (PwD) account for at least 10% of any given population [5] and exhibit traits that may negatively impact on their password management practices [6]. We know that individuals with dyslexia face concrete problems navigating the online

world [7] with many online communications relying on text-based interactions. While audio-visual content continues to proliferate in online platforms, we continue to see a reliance on text-based authentication despite more usable methods such as pattern unlock and biometric recognition being pushed on mobile devices.

In this paper, we focus on understanding the user authentication experiences of PwD and explore the acceptability of graphical passwords – alternatives to alphanumeric solutions that rely on image recognition or pattern generation [8] rather than on textual recall or spelling. We do this through interactive interviews where participants were encouraged to try three different authentication systems and then discuss their strategies behind code composition. This paper makes two distinct contributions: (i) To the best of our knowledge, this is the first paper to explore PwD's experiences of graphical versus alphanumeric authentication schemes in everyday life, and (ii) this work is the first to explore the acceptability of graphical passwords amongst the PwD population.

2 Background

2.1 Computer Users with Dyslexia

Dyslexia is a common neurological and often hereditary learning disability [9]. The prevalence of dyslexia in any given population is not insignificant, with estimates suggesting at least 10% of individuals show symptoms associated with the disability [5]. In the UK, it is estimated that 4% of the population exhibit severe symptoms [10].

Individuals with dyslexia exhibit trouble recognising phonemes and connecting the sounds with the symbols denoting the letters. As such, a word can be misspelled in various different ways by the same user, for example "dalb" and "pald" as variations to "bald". Further, blending sounds into words may be a pronounced difficulty, for example reading and understanding a word correctly, but being unable to read it aloud as it does not compute correctly, resulting in a pronunciation latency. Some people with dyslexia may also exhibit errors regarding semantically-related words: "parrot" for "canary", for example [11]. As a result, people with dyslexia have noticeable trouble reading and spelling, which has been shown to affect day to day online communication [7]. In particular, they have been known to avoid using services that require precise spelling despite being regarded as more trustworthy [12] and avoid combining sources due to working memory limitations [13], which indicates that workarounds are employed by this population in order to overcome systems that rely on textual interactions.

2.2 User Authentication and Graphical Passwords

Passwords, the most common form of user authentication for digital accounts, have also been reported to be problematic for PwD, in particular requiring users to spend longer entering passwords when logging in and the resulting passwords being easier to guess [14]. However, issues with password management are not exclusive to PwD: Users notably engage in insecure practices due to optimistic cognitive biases, or by

overlooking immediate consequences, or simply because the trade-off between security and convenience is better in the short term [15, 16]. Often the case is that the users are experiencing a so-called security fatigue [17], which results in a lack of security conscious in daily dealings in the online world, particularly when relating to passwords. Some of the most common issues are creating overly simple and personalised – hence guessable – codes [18], using the same code for more than one account [19], and sharing the codes with friends and family [15].

With these limitations in mind, researchers have looked at other forms of knowledge-based authentication such as challenge questions [20] and graphical authentication systems [8, 21, 22]. Graphical passwords are of particular interest, as we have seen that user groups who typically struggle with either declining cognitive function or with the usability aspects of technology can find this type of authentication suitable: for example, previous work has demonstrated how older users [22] and users with learning difficulties [23] can benefit from the affordances of graphical passwords. This improved performance is in part due to the graphical mechanism bypassing reading and spelling issues, as well as supporting the memorability (e.g. through cued-recall or recognition) of the codes [8]. While issues with scalability have resulted in alphanumeric passwords remaining as the de-facto authentication method for most services, graphical passwords may become a more realistic prospect for both service providers and end users with the proliferation of devices with higher resolution, touch screens, and faster data access.

2.3 Design

The study consisted of semi-structured interactive interviews with internet users with dyslexia (see Figure 1). Participants were asked to create authentication codes using a bespoke prototype to enable an informed and immersed interview, but the key findings reported here focus on the thematic analysis [24] of the qualitative data (see 2.6 for details). We recruited 6 participants who reported being diagnosed with dyslexia aged between 18 and 25 years with a 1:1 male-female ratio. Due to ethics procedures, the severity of dyslexia symptoms was not recorded. Participants were recruited through email calls circulated within our institution and through snowball sampling, resulting in all participants being either undergraduate or postgraduate students.

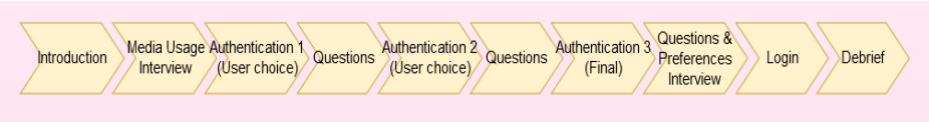

Figure 1: The interactive interviews consisted of several activities and open-ended questions.

2.4 Materials

In order to understand the user authentication experiences of PwD, we developed a bespoke local website that incorporated three different authentication schemes: an

alphanumeric password, a PIN, and a graphical password. The alphanumeric password and PIN implementation consisted of the standard text fields for input. Most apps and websites support the alphanumeric password as the default, if not the only, option for authentication, thus a real-time observation of the user experience with it was the prudent first step in the study. This furthermore served as a 'baseline' of comparison in terms of participant reaction. The PIN was chosen in consideration of the fact that it is a key part of several daily life activities such as banking, physical access devices, and notably even some websites. The graphical password was a simple image pattern cued-recall password similar to Cued Click Points [21] consisting of an image with an overlay of selectable squares that divide the image into sections, any number of which could be selected to create a unique code (see Figure 2 below). Given the exploratory nature of this work, the interview structure was designed to elicit the mental models of participants with regards to authentication mechanisms as well as to encourage

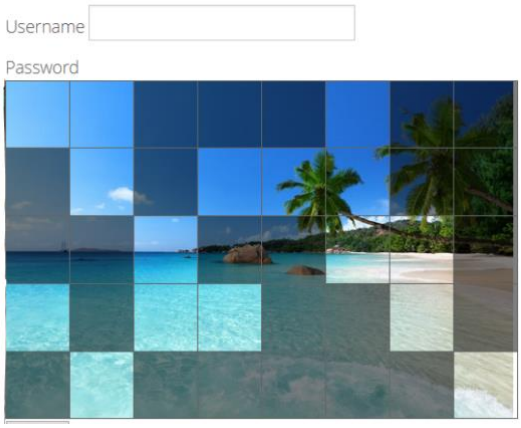

Figure 2: An example of a code created on the prototype graphical password.

discussion around habits for code creation (see 2.5 below).

2.5 Procedure

The interview was designed around the task of creating the various types of passwords following a basic structure of create-distract-authenticate (see Figure 1). First, the participants were asked about their general habits of creating accounts on social media to collect initial behavioural insights. Then, they were tasked with creating an account on the website tool using one mechanism of their choice and their steps and choices were observed while being encouraged to narrate their steps [25]. Participants were asked to follow the steps taken to create a code for a social media website. Following the account creation, participants were asked to reflect on their pick of mechanism and code with some follow-up questions, with a general question about their security consciousness at the end to serve as a distractor task. Participants then followed the same procedure for the other two authentication mechanisms. Once all accounts had been created, they were asked about their experience with dyslexia and online authentication. Finally, participants were asked to authenticate on the website

using the same code they devised previously in order to ascertain whether the credentials were memorable (i.e., realistic) within a short time period. In total, the average time taken to complete the interactive interviews, which consisted of 8 open-ended questions, was 30 minutes. This study was approved by our institution's Ethics Committee.

2.6 Data Analysis

All interviews were audio recorded and transcribed. Then, all transcribed data was analysed using thematic analysis, (e.g. [24]) following the five stages of familiarization, the identification of a thematic framework, indexing, charting, and interpretation. The two members of the research team worked on the data and ensured agreement on the framework and subthemes before they were finalised. We note that the analysis was carried out on all qualitative data collected throughout the interactive interview (including the talk aloud) and not just the pre-defined questions.

3 Results

Here we report on the themes we identified related to user experiences of authentication and dyslexia. Below, we describe in more detail the themes of Familiarity, Effort, and Patterns. First, however, we discuss some similarities that our participants shared with well-known password management behaviours reported in the literature.

3.1 Poor Password Management Behaviours

Supporting vast amounts of previous work reporting on the poor password management behaviours of the general population [15, 16, 18, 19], our participants reported a number of concerning security behaviours and mental models. In particular, the majority of our participants reported reusing their passwords across many platforms, created short passwords, and/or used personal information (e.g., birthdays and names) in their passwords. This is a significant risk for password security as passwords constructed using these characteristics can be very vulnerable to probabilistic context-free grammars (PCFGs) password cracking methods [26].

When analysing the alphanumeric passwords that were created for the password condition in our study, we see that passwords were between 8 and 15 characters. None of the created passwords included special characters, and 5/6 of the passwords included one or more simple dictionary words that would be picked up with a basic dictionary attack. Despite these clear issues, the absence of any historical consequences demotivated participants from changing these behaviours:

"Not really when creating them apart from the fact that the ones I'm making probably aren't that secure. But I've gotten away with having short probably not that secure ones." – Participant 3.

Participants all reasoned that they had not been attacked so far, or that they do not hold any information they deem significant enough to be worried about in their online

accounts. This self-fulfilling prophecy is not uncommon with security behaviours and is in line with the studies demonstrating how users generally know and understand good security practices but do not employ them due to a cognitive bias imposed by the lack of immediate negative consequences [16].

3.2 System Familiarity

It was clear from our observations of participants using the three authentication mechanisms that they gravitated towards familiar systems (passwords and PINs) and avoided the unknown system (graphical password).

While our participants were not put off by the graphical password specifically, they preferred erring on the side of the known when they were given an option of mechanism. This behaviour indicates that implementing alternative, more secure and potentially dyslexia-friendly technologies for authentication may be difficult as users would default to the current standard if given a choice. The Technology Acceptance Model (TAM) [27] describes how the perceived usefulness of a system has a significant positive correlation to the actual system use over the perceived ease of use. For an authentication system, this means that its usability and security need to be perceived as being a significant upgrade over traditional alphanumeric passwords to bypass existing defaults, something which is not immediately apparent with graphical passwords.

"That's just a waste of time. I'd rather just type something in because I type faster than I fiddle around. And most of the time when you're doing it, you're going to have a problem where it's going to miss where you dragged, or link somewhere else, or click somewhere else. (...) It's just long." – Participant 5.

As the participant above explains, without much context a graphical password seems like a suboptimal choice for users who are used to authenticating using alphanumeric passwords. However, as discussed in the following subsection, we can begin to see how graphical password may actually be of benefit for PwD and their opinions towards these mechanisms began to improve after use.

3.3 Patterns

A common theme across strategies employed by participants when creating text-based authentication codes was the use of patterns. Our participants reported relying on patterns generated using the keyboard or other input device rather than relying on the actual content of the code.

"If you asked me to tell it to you, I wouldn't be able to. It's a pattern on my keyboard, the same with my work password that I use at work. I don't know the number; I just know where I put my fingers on the keyboard." -Participant 3.

Users employing patterns in passwords is not a new finding [28], but the sheer over-reliance in patterns reported (and observed) by our sample suggests that young PwD may utilise this as a primary technique for key accounts. This is not necessarily surprising, as the disregard of a heavy memory task in favour of the reportedly easier visuospatial pattern [29] seems to make sense.

"I'm trying to make one [password] based on my visual again, rather than making one up that… If I just pick some numbers, I'll forget them." – Participant 3.

The participant above touches on a particular problem that users face when relying on patterns when creating passwords: visual patterns on keyboards are limited, and well-known to cyber criminals. For example, we know that many users rely on simple patterns such as qwerty, qazxsw, and the most popular password 123456 [30], while criminals seek out these patterns when configuring mangling rules for password cracking. As such, PwD who may have an over-reliance on patterns for password creation could be at a higher risk of having them revealed in cyber-incidents.

On the other hand, once participants had an opportunity to create a code using the graphical password, they begun to see the benefits of this scheme. In particular, the fact that the scheme we chose encouraged pattern recognition.

"I think it would be easier just to remember a pattern over specific parts of an image. It was quite basic for me to remember where the squares were on the image." - Participant 5.

While this realisation can be positive for system adoption, an over reliance on basic patterns could also be problematic for graphical passwords. When our participants were given the option to create a code using the graphical password, they mostly picked simple, easy to remember and recreate patterns: a smiley face, a checkerboard pattern, or salient points on the given image such as the shore or the trees. These patterns are not only easily reproducible for the user, but also for any potential attacker [31], which is an undesirable outcome. However, we must note that our participants were not given any prior information about graphical passwords and they were not creating these passwords for valuable personal accounts, so there is scope for future work to understand the types of patterns that are used in high-stakes situations.

3.4 Effort

Participants commonly reported taking extra steps to minimise the effects of dyslexia on their authentication experiences. In particular, participants reported taking extra time to authenticate in order to avoid errors.

"I cannot say, but I do take pauses just to make sure I'm typing the correct numbers and it makes sense to me." -Participant 6.

The participant above further elaborated that sometimes it takes them extra tries because they mistook a 1 for an "l", or they mistyped a number and it would take them a while to find it. This is in line with previous work reporting on the delay in authentication attempts when using alphanumeric passwords [14]. Another participant displaying the typical confusion with "b" and "d," "p" and "q" when reading, reported that such issues typically resulted in slower logins rather than more logins.

The observation that individuals with dyslexia expect to take longer to authenticate can be beneficial for graphical password schemes. The longer login times are often cited as being one of the key issues around adoption [8], yet user groups like PwD and older adults, who usually take longer to authenticate anyway, may not see this as a problem and in fact actual differences in time may not be as pronounced.

4 Discussion

In this study we explored how individuals with dyslexia engaged with authentication mechanisms including alphanumeric and graphical passwords, and reported on how graphical passwords have the potential to serve as inclusive authentication mechanisms for PwD. In particular, we note how PwD take longer to authenticate using passwords and rely on patterns for their codes. This extra login time has traditionally been seen as an obstacle for adoption for graphical passwords [8], yet previous work [14] and our own findings highlight how users with dyslexia take extra time when entering passwords in order to avoid mistakes: this means that in practice the time taken to enter a *strong* password and the time taken to select a pattern on a graphical password may not be as pronounced for this user group.

4.1 Pattern-Based Code Composition

While our participants appreciated the mechanics of the graphical password we tested, which facilitated the use of patterns [21] in the composition of the code, it remains to be seen how PwD may approach other types of graphical passwords – most notably recognition-based systems that do not feature pattern recognition at all. Further investigation into the types of patterns that are generated by users with dyslexia when using graphical passwords is also warranted to ensure that these are not prone to hotspot attacks [31].

However, it is important to also take into consideration how we might approach this population's over-reliance on patterns in the composition of knowledge-based codes. While this insight originates from only six participants – all of which were university students – we know from research into the general population that patterns are a method for creating weaker passwords [28]. Additionally, the insights obtained from our individual participants appear to suggest that the use of patterns as a composition strategy across many accounts serves as a workaround for their well-documented issues with spelling [11] which deserves further inquiry.

4.2 Conclusion

This paper has presented some initial insights on the approaches that users with dyslexia employ when evaluating authentication systems and the potential acceptability of graphical passwords for PwD. Building on other work demonstrating how this type of authentication can benefit marginalised user groups (e.g. older adults [22]), we begin to explore whether graphical passwords could be used as an additional choice to alphanumeric passwords to benefit specific users groups by improving memorability [8] while removing some of the problematic text-based issues that this population faces [11]. We posit that this line of enquiry could be promising but more work is needed to understand how to communicate the benefits to these users in a clear but inclusive way.

References

1. Meyer, B.: COMB: over 3.2 Billion Email/Password Combinations Leaked, https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free/
2. Stobert, E., Biddle, R.: The Password Life Cycle. ACM Trans. Priv. Secur. 21, 13:1-13:32 (2018). https://doi.org/10.1145/3183341
3. National Cyber Security Centre: Password Guidance: Simplifying Your Approach. National Cyber Security Centre
4. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X.: The Tangled Web of Password Reuse. Presented at the NDSS (2014)
5. Sprenger-Charolles, L., Siegel, L.S., Jiménez, J.E., Ziegler, J.C.: Prevalence and Reliability of Phonological, Surface, and Mixed Profiles in Dyslexia: A Review of Studies Conducted in Languages Varying in Orthographic Depth. Scientific Studies of Reading. 15, 498–521 (2011). https://doi.org/10.1080/10888438.2010.524463
6. Renaud, K., Johnson, G., Ophoff, J.: Dyslexia and Password Usage: Accessibility in Authentication Design. In: Clarke, N. and Furnell, S. (eds.) Human Aspects of Information Security and Assurance. pp. 259–268. Springer International Publishing, Cham (2020)
7. Kanniainen, L., Kiili, C., Tolvanen, A., Aro, M., Leppänen, P.H.T.: Literacy skills and online research and comprehension: struggling readers face difficulties online. Read Writ. 32, 2201–2222 (2019). https://doi.org/10.1007/s11145-019-09944-9
8. Biddle, R., Chiasson, S., Van Oorschot, P.C.: Graphical passwords: Learning from the first twelve years. ACM Comput. Surv. 44, 19:1-19:41 (2012). https://doi.org/10.1145/2333112.2333114
9. Snowling, M.J., Gallagher, A., Frith, U.: Family Risk of Dyslexia Is Continuous: Individual Differences in the Precursors of Reading Skill. Child Development. 74, 358–373 (2003). https://doi.org/10.1111/1467-8624.7402003
10. British Dyslexia Association: Dyslexia, https://www.bdadyslexia.org.uk/dyslexia
11. Baddeley, A.D., Logie, R.H., Ellis, N.C.: Characteristics of developmental dyslexia. Cognition. 29, 197–228 (1988). https://doi.org/10.1016/0010-0277(88)90024-8
12. Kvikne, B., Berget, G.: When Trustworthy Information Becomes Inaccessible: The Search Behaviour of Users with Dyslexia in an Online Encyclopedia. IOS Press (2018)
13. Andresen, A., Anmarkrud, Ø., Bråten, I.: Investigating multiple source use among students with and without dyslexia. Read Writ. 32, 1149–1174 (2019). https://doi.org/10.1007/s11145-018-9904-z
14. Helkala, K.: Disabilities and Authentication Methods: Usability and Security. In: 2012 Seventh International Conference on Availability, Reliability and Security. pp. 327–334 (2012)
15. Whitty, M., Doodson, J., Creese, S., Hodges, D.: Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. Cyberpsychology, Behavior, and Social Networking. 18, 3–7 (2014). https://doi.org/10.1089/cyber.2014.0179
16. Tam, L., Glassman, M., Vandenwauver, M.: The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology. 29, 233–244 (2010). https://doi.org/10.1080/01449290903121386
17. Stanton, B., Theofanos, M., Spickard Prettyman, S., Furman, S.: Security Fatigue. IT Professional. 18, 26–32 (2016). https://doi.org/10.1109/MITP.2016.84

18. Ur, B., Noma, F., Bees, J., Segreti, S.M., Shay, R., Bauer, L., Christin, N., Cranor, L.F.: 'I Added "!" at the End to Make It Secure': Observing Password Creation in the Lab. Presented at the Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) (2015)
19. Wash, R., Rader, E., Berman, R., Wellmer, Z.: Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites. Presented at the Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016) (2016)
20. Just, M., Aspinall, D.: Personal choice and challenge questions: a security and usability assessment. In: Proceedings of the 5th Symposium on Usable Privacy and Security. pp. 1–11. Association for Computing Machinery, New York, NY, USA (2009)
21. Chiasson, S., van Oorschot, P.C., Biddle, R.: Graphical Password Authentication Using Cued Click Points. In: Biskup, J. and López, J. (eds.) Computer Security – ESORICS 2007. pp. 359–374. Springer, Berlin, Heidelberg (2007)
22. Nicholson, J., Coventry, L., Briggs, P.: Age-related performance issues for PIN and face-based authentication systems. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 323–332. Association for Computing Machinery, New York, NY, USA (2013)
23. Marne, S.T., Al-Ameen, M.N., Wright, M.: Learning System-assigned Passwords: A Preliminary Study on the People with Learning Disabilities. Presented at the Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017) (2017)
24. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative Research in Psychology. 3, 77–101 (2006). https://doi.org/10.1191/1478088706qp063oa
25. Ericsson, K.A., Simon, H.A.: Verbal reports as data. Psychological Review. 87, 215–251 (1980). https://doi.org/10.1037/0033-295X.87.3.215
26. Li, Y., Wang, H., Sun, K.: Personal Information in Passwords and Its Security Implications. IEEE Transactions on Information Forensics and Security. 12, 2320–2333 (2017). https://doi.org/10.1109/TIFS.2017.2705627
27. Davis, F.D.: User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. International Journal of Man-Machine Studies. 38, 475–487 (1993). https://doi.org/10.1006/imms.1993.1022
28. Shay, R., Komanduri, S., Durity, A.L., Huh, P. (Seyoung), Mazurek, M.L., Segreti, S.M., Ur, B., Bauer, L., Christin, N., Cranor, L.F.: Can long passwords be secure and usable? In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2927–2936. Association for Computing Machinery, New York, NY, USA (2014)
29. Schnotz, W.: An Integrated Model of Text and Picture Comprehension. In: Mayer, R. (ed.) The Cambridge Handbook of Multimedia Learning. Cambridge University Press (2005)
30. NordPass: Top 200 Most Common Passwords of 2020, https://nordpass.com/most-common-passwords-list/
31. Thorpe, J., van Oorschot, P.C.: Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. Presented at the 16th USENIX Security Symposium (2007)