

JYX



JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Woods, Naomi; Silvennoinen, Johanna

Title: Enhancing the user authentication process with colour memory cues

Year: 2023

Version: Published version

Copyright: © 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis

Rights: CC BY-NC-ND 4.0

Rights url: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

Please cite the original version:

Woods, N., & Silvennoinen, J. (2023). Enhancing the user authentication process with colour memory cues. *Behaviour and Information Technology*, 42(10), 1548-1567.

<https://doi.org/10.1080/0144929x.2022.2091474>



Enhancing the user authentication process with colour memory cues

Naomi Woods & Johanna Silvennoinen

To cite this article: Naomi Woods & Johanna Silvennoinen (2022): Enhancing the user authentication process with colour memory cues, Behaviour & Information Technology, DOI: [10.1080/0144929X.2022.2091474](https://doi.org/10.1080/0144929X.2022.2091474)

To link to this article: <https://doi.org/10.1080/0144929X.2022.2091474>



© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 15 Jul 2022.



Submit your article to this journal [↗](#)



Article views: 31



View related articles [↗](#)



View Crossmark data [↗](#)

Enhancing the user authentication process with colour memory cues

Naomi Woods and Johanna Silvennoinen

Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland

ABSTRACT

The authentication process is the first line of defence against potential impostors, and therefore is an important concern when protecting personal and organisational data. Although there are many options to authenticate digital users, passwords remain the most common authentication mechanism. However, with password numbers increasing, many users struggle with remembering multiple passwords, which affects their security behaviour. Previous researchers and practitioners have attempted to suggest ways to improve password memorability and security simultaneously. We introduce novel approach that utilises colour as a memory cue to increase password memorability and security. A longitudinal study examined in total over 3000 passwords that were created, learnt and recalled (password process) over a period of five-weeks. By adding colour to the password process, our results suggest that password memorability and security can be increased simultaneously. Through giving the user the option of choosing the colours (compared with colours being preselected), encourages users to create more personal and meaningful memory cues when creating their passwords. Additionally, colour also provided another security parameter by increasing password entropy. These unique results have practical implications for researchers and practitioners that could positively impact password security, and the financial losses suffered due to password security breaches.

ARTICLE HISTORY

Received 12 January 2022
Accepted 14 June 2022

KEYWORDS



Authentication; password memorability; memory cues; colour; colour preference; security behaviour

1. Introduction

Users have a variety of different digital accounts and systems holding personal and organisational information, from medical records, to financial information. Gaining access to these accounts and systems not only gives the user access to view information (potentially sensitive and important information), but it can also allow the user to perform actions, such as financial transactions, and communicating, such as emails and using social media (Bang et al. 2012; Vu et al. 2007). Text-based password authentication is one of the most prevalent ways to secure these systems and accounts within organisations and within users' personal lives (Florêncio and Herley 2010; Keith, Shao, and Steinbart 2009; Seitz et al. 2017; Ur et al. 2016; Wang et al. 2016; Yang et al. 2016). However, the user is undermining the current authentication mechanism (Grawemeyer and Johnson 2011; Zhang et al. 2009). With widespread technology usage being an integral part of most people's life (Legner et al. 2017), the number of accounts and systems has exponentially increased. This is resulting in users struggling to remember all their passwords, and adopting insecure password

behaviours, choosing memorability and/or convenience over password security (Grawemeyer and Johnson 2011; Tam, Glassman, and Vandenwauver 2010; Weir et al. 2009; Zhang et al. 2009). Users will adopt insecure password behaviours such as choosing weak passwords, reusing passwords, writing passwords down and storing them in an unsecured way (Adams and Sasse 1999; Campbell, Kleeman, and Ma 2006; Inglesant and Sasse 2010; Merdenyan and Petrie 2022; Seo and Park 2019; Zhang et al. 2009). Insecure password behaviours lead to a significant amount of money being lost and spent on security breaches (Brown et al. 2004; Ives, Walsh, and Schneider 2004; Mamonov and Benbunan-Fich 2018; Vu et al. 2007). Besides insecure password behaviours, the consequences of forgetting passwords are also expensive, with organisations spending thousands to millions of dollars on resetting passwords (Brostoff and Sasse 2000; Brown et al. 2004; Hayashi et al. 2012; Ives, Walsh, and Schneider 2004; Saastamoinen 2014; Vu et al. 2007).

Even with all the problems that the current password mechanism brings, there is no adequate alternative to replace them (Bonneau and Preibusch 2010; Herley

CONTACT Naomi Woods  naomi.woods@jyu.fi  Faculty of Information Technology, University of Jyväskylä, P.O. Box 35 (Agora) FI-40014 Jyväskylä, Finland

© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

and Van Oorschot 2012; Pasquini et al. 2021; Wang et al. 2019). For example, several studies have found that even though password manager software has existed for several decades, they are not widely accepted. Previous studies have found that users would prefer to memorise their passwords, instead of using password managers (Das et al. 2014), and even when encouraged to use them, users still prefer not to (Alkaldi, Renaud, and Mackenzie 2018). The reasons for not using password managers are due to trust (users believe they are vulnerable to attacks and prefer to trust their own memory) (Gaw and Felten 2006); usability (Chiasson, van Oorschot, and Biddle 2006); and that they cannot be used for all systems, accounts and devices. Another example is that despite the advances in biometric mechanisms (Renaud and De Angeli 2009), biometrics have still not replaced passwords (Florêncio and Herley 2010; Keith, Shao, and Steinbart 2009). Biometrics have their disadvantages: cost (new technology, and changing systems), usability (constraints from screen size), habit and familiarity (users place trust in it) (Florêncio and Herley 2007; Kharrufa, Ploetz, and Olivier 2017); and like password managers, they cannot be used for all systems and accounts. Therefore, it is imperative to find ways to increase password memorability whilst not significantly impacting their security or the convenience of the process (Grawemeyer and Johnson 2011; Woods and Siponen 2018; 2019).

To address the trade-off between password memorability and security, in this study we utilise colour as a memory cue in the process of creating, learning and recalling passwords. Several studies have shown that colour can increase memorability (Helkala and Svendsen 2011; Hanna and Remington 1996; Huang, Lin, and Chiang 2008); however, it has not been examined in the password security context. Therefore, through a longitudinal experimental study of password recall, we apply colour to the password authentication process and argue that password memorability can be increased, along with security by means of an additional colour parameter. In the next section, we will review the literature related to password memorability and security. We then will examine the memory theories that support the use of colour as a memory cue for password memorability, supporting our hypotheses. The following sections will next discuss the methodology and results. Finally, the paper will conclude with a discussion of the study's results, their contributions and implications.

2. Theoretical background and hypotheses

With the introduction of the internet and smart technologies over the past few years, technology has spread

to every part of users' lives (Woods 2022). Nowadays, there are over 4.3 billion internet users (World Internet Users Statistics 2019), and each user is thought to have on average over 25 text-based passwords each (Florêncio and Herley 2007). Most users are struggling to cope with remembering all their passwords, which is leading to much frustration (Herley and Van Oorschot 2012; Ryan and Valverde 2006) and the use of insecure security behaviours (Adams and Sasse 1999; Campbell, Kleeman, and Ma 2006; Guo 2013; Herley and Van Oorschot 2012; Hoonakker, Bornoe, and Carayon 2009; Inglesant and Sasse 2010; Marquardson 2012; Zhang et al. 2009). Many years ago, password authentication systems were developed with little consideration of the sheer numbers we see today, nor with understanding of how the user will be able to cope with these numbers, psychologically and cognitively (Adams and Sasse 1999; Grawemeyer and Johnson 2011; Furnell, Helkala, and Woods 2022; Woods 2017; Woods and Siponen 2018; 2019). Therefore, understanding the user's cognitive and psychological processes and the user's interaction with password security is imperative to ensure the security of the user.

2.1. The trade-off between password memorability and password security

Previous research has examined password security, approaching the issues from a behavioural perspective. Though considering that non-compliance to password security policies have similar causalities as non-compliance to other (more general) security policies; and therefore, should be treated the same. These studies apply behavioural theories such as deterrence theory, protection motivation theory and fear appeals to suggest ways to improve password security behaviour (Guo and Yuan 2012; Herath and Rao 2009; Jenkins et al. 2014; Johnston, Warkentin, and Siponen 2015; Shay et al. 2015; Siponen and Vance 2014; Vance et al. 2013; Workman, Bommer, and Straub 2008). However, these theories do not take into account the users' memory and its effects on password security behaviour (Woods and Siponen 2018; 2019). Insecure password behaviors stem mainly from users being unable to remember large numbers of passwords (Florêncio and Herley 2010; Gaw and Felten 2006; Notoatmodjo and Thomborson 2009). Therefore, there is a plethora of research examining the effects of the human memory on password security. These studies have identified a trade-off between password memorability and security, as users will choose weaker passwords because they feel that including a word or some personal information will make them more memorable (Das et al. 2014; Habib

et al. 2018; Sasse, Brostoff, and Weirich 2001). Users will write down their passwords and store them in an insecure manner, for example, an unencrypted document on their computer or mobile phone, as they feel they are incapable of remembering all their passwords (Campbell, Kleeman, and Ma 2006; Das et al. 2014; Nelson and Vu 2010; Wiedenbeck et al. 2005). Furthermore, users will reuse and modify their passwords, as they believe it will help them remember them more easily, and that creating new passwords is difficult to learn (Adams and Sasse 1999; Campbell, Kleeman, and Ma 2006; Guo 2013; Zhang et al. 2009). Several studies have also applied techniques (including memory techniques) and technologies to password management (Al-Ameen, Wright, and Scielzo 2015; 2020; Forget, Chiasson, and Biddle 2008; Haque et al. 2017; Hartwig and Reuter 2021; Masui 2013; Peer et al. 2020; Stobert and Biddle 2014; Woo et al. 2019; Yang et al. 2016; Zhang et al. 2009). However, attempting to strike a balance or simultaneously improve both memorability and security is a difficult task, as often one factor will suffer (Woods and Siponen 2018; 2019).

2.2 . Memory, retrieval and memory cues

Many researchers have turned to psychology and cognitive science to understand how the human memory effects password memorability (e.g. Gao et al. 2018; Nelson and Vu 2010; Stobert and Biddle 2014; Wiedenbeck et al. 2005; Woods and Siponen 2018; 2019). According to Atkinson and Shiffrin (1968), their multi-store memory model proposed three memory stores, where information is first received and processed through the sensory store. The information is then briefly held and processed in short-term memory (STM) or working memory (WM) (updated in 1974) (Baddeley and Hitch 1974), where the information is coherently combined from all sensory channels and encoded. It is then transferred to long-term memory (LTM) for long-term storage and retrieval.

When encoding (or learning) information, the more deeply the information is processed, by processing it on several levels (such as verbally and visually) and through adding meaning, the better it is retained (Craik and Lockhart 1972). Moreover, dual-coding theory proposes that visual and verbal information is processed on different channels, and therefore if the information has both types it will increase the levels of processing (Paivio 1971). Likewise, through attaching information that has already been learnt (stored in LTM) to the information that is being learned, this too will increase memorability and retrieval; this is referred to elaborative processing (Craik and Lockhart 1972).

When attempting to remember information, retrieval from LTM will start with one or more memory cues that will activate all associated memory traces to bring the target memory into awareness. This process can fail when memory cues are weak or inappropriately associated with the target memory, and when not enough effort is paid to the retrieval process (Anderson 2009). Nevertheless, when failure occurs, it does not mean that the memory is lost; failure to retrieve a memory can also be attributed to the context, such as the environment and/or emotional state of the person (Anderson 2009). However, the stronger and more appropriate the memory cue/s are related to the target memory, and the more attention that is devoted in retrieving the target memory, the better chance of success (Baddeley 2009a). Furthermore, due to encoding specificity principle, the more similar the retrieval cues are when recalling a target memory, to that of the conditions available at the encoding stage, the more successful the retrieval will be (Tulving and Thomson 1973).

Memory cues or retrieval cues are little bits of information that can be used as a prompt or hint to access a memory stored in LTM (Anderson 2009). They can include visual and/or verbal information, for example in the form of a question, ‘what did you do at the weekend?’ or they can be just one word, such as ‘house’, they can be in the form of a picture, or being just one note of music. They can also be merely a smell, or be the environmental context or an emotional context. Regardless of their form, more memory cues lead to easier access to the target memory (Anderson 2009; Hanna and Remington 1996).

2.3. Colour as a memory cue

Colour can be used as a meaningful memory cue for retrieving target information (Hanna and Remington 1996; Helkala and Svendsen 2012; Huang, Lin, and Chiang 2008). Colour is processed independently to any other visual sensory information e.g. motion and depth, through an area of the visual cortex dedicated to processing just colour (Hanna and Remington 1996; Livingstone and Hubel 1987; Zeki 1993; Zeki and Marini 1998). It operates as an influential information channel to the human cognitive system, and functions as a significant source in improving memory performance (Wichmann, Sharpe, and Gegenfurtner 2002). Previous studies have shown that participants perform better at memory tests when colour is present as a cue (Hanna and Remington 1996). Due to the effectiveness of colour, it is often seen as a primary visual element that can add interest in any visual context

(e.g. Poulin 2011). Coloured information results in better attention and memorability than information with an achromatic colour scheme (Farley and Grant 1976; Wichmann, Sharpe, and Gegenfurtner 2002). This is because colour can add meaning to a memory when it is being encoded (Derefeldt et al. 2004; Huang, Lin, and Chiang 2008).

Colour preferences have also been found to have an effect on memory and can affect the way information is processed (Huang, Lin, and Chiang 2008; Palmer and Schloss 2010). Maier et al. (2009) found strong preferences for the colour red, over colours such as green and grey. However, colour preferences can differ between cultures (Taylor, Clifford, and Franklin 2013). Previous studies have also found a strong valence between colours and objects/contexts, ‘People like colours strongly associated with objects they like (e.g. blues with clear skies and clean water) and dislike colours strongly associated with objects they dislike (e.g. browns with faeces and rotten food)’ (Palmer and Schloss 2010, 107). Colour preference and selection enhances memorability due to the increase in the depth of processing (Craik and Lockhart 1972; Huang, Lin, and Chiang 2008), and due to the way it can increase the visual working memory capacity similar to reward-incentive motivations (Kawasaki and Yamaguchi 2012). Furthermore, colour can utilise the encoding specificity principle, contributing to the retrieval process if present at the encoding stage (Hanna and Remington 1996).

2.4 . Colour used in security

Previous research has suggested that colour as a memory cue can be used in various ways to increase security. A recent study has found that colour can be used as a part of a filter to add privacy to password management (Khamis et al. 2019); colour has also been used to aid the memory of passwords in a graphical password scheme (Chiang and Chiasson 2013). Several studies have applied colour to other graphical password options such as digital signatures as a form of authentication (Thoopsamut and Limthanmaphon 2019), and drawmetric graphical passwords such as Passdoodle and Pass-Go (Biddle, Chiasson, and Van Orschot 2012). By adding the colour to the pen in these drawmetric graphical passwords, it enhances personalisation, variability and complexity through the additional parameter, which can increase security (Biddle et al. 2012; van Orschot and Thorpe 2008). A study by Renaud and Ramsey (2014) examined the memorability of PIN codes through using pre-selected colours. Although, they found that through adding colour, the

memorability of the PIN codes was not increased. These unexpected findings could have been due to that the colours were pre-selected by the experimenters; colour research has shown that preferences and selection of colour can affect memory accuracy (Huang, Lin, and Chiang 2008). Colour has been suggested as a memory cue to increase text-based passwords memorability. Helkala and Svendsen (2012) proposed that an ‘associated element’ such as a colour, a shape, text or an element associated with the service (e.g. present on the internet page), could be used as a memory cue, and incorporated into creating text-based passwords. The associated elements were incorporated in the form of the name of the element (e.g. golden, or circle) as a part of the actual password ‘TringleCirclePrincess-WithGoldenBl’. They found that including these elements in this way increased password memorability.

2.5. Current study

Drawing upon memory theory and specifically with regard to colour memory cues, we have developed a novel approach to examine colour cues in the security context that is different to what has been studied previously. PIN entry is much different from that of complex text-based passwords, due to passwords’ complex nature in terms of length, character composition and meaning to the user. Thus, making strong colour associations between a random four-digit number maybe more difficult (Renaud and Ramsey, 2014), than with a complex text-based password. Moreover, applying colour to drawmetric graphical passwords would also be different compared with text-based passwords. This is because the cognitive process is different to that of processing simple one line drawn graphical passwords. With additional levels of memory processing through the complexity of text-based passwords (Craik and Lockhart 1972), plus the addition of colour, this could consequently produce stronger memory cues, for enhanced password retrieval. Therefore, in this study, we propose adding colour to text-based passwords can be utilised as a memory cue to increase password memorability, and as an additional parameter to increase password security, simultaneously. Hence, we hypothesise:

H1: Coloured passwords will have a positive effect on correct password recall, compared with passwords with no colour.

Colour selection in the password creation process will add another cognitive processing stage, which increases the depth of processing (Huang, Lin, and Chiang 2008), which enhances the memorability of the created password. We therefore, hypothesise:

H2: Personally selected colours will have a greater positive effect on memorability of colours than preselected colours.

H3: Personally selected colours will have a greater positive effect on correct password recall, compared with passwords with preselected colour and passwords with no colour.

3. Research methods

A longitudinal study was designed based on several previous password studies. The participants created, learnt and recalled passwords several times over five weeks. During the experiment, data were collected to measure password recall, and the effects of colour as a memory cue for recalling passwords.

3.1. Participants

Previous studies have found that when comparing passwords collected from participants who were workers to those who were staff and students from universities, it has been noted that there is very little difference between the two groups (Mazurek et al. 2013; Shay et al. 2016). Therefore, we selected 90 participants from staff and students from a European university. All participants were all experienced computer users and were employed. Participants exhibiting any colour blindness were prohibited from taking part in the study, as it could have potentially affected the results. Although they could not take part, it would not mean that users with colour blindness could not use colour as a part of their authentication process. All the colours were checked for accessibility using an accessibility colour checker (<https://webaim.org/resources/contrastchecker/>) to make sure they were all considered WCAG 2.0 level AA accessible for graphical objects and user interface components. All the colours passed apart from one – light orange. We chose to keep this colour in the selection to give more variability for those without any issues, and had chosen to not change the hue as it

would have been too similar to the darker version of the colour. Those users who are colour blind would use the colours available that were not an issue for their colour perception. The participants' colour blindness was tested in the recruitment stage by two colour blindness tests. The sample size required to achieve a good level of statistical power (0.80) (Cohen 1992) was assessed before recruitment, and was surpassed by 90 participants being allocated to three groups: control (no colour) group ($N = 30$); preselected colour group ($N = 30$); and the personally selected colour group ($N = 30$). All groups were matched for age, as age can affect memory (Baddeley 2009b). Demographic information is reported in Table 1. To encourage participants to engage and complete the study, a movie ticket was offered as an incentive for their participation.

3.2. Measures

Recruitment: During the recruitment process, participants were asked to take two colour blindness tests, employed to identify participants with colour blindness. The first was an Ishihara Test, consisting of several colour plates containing coloured randomised dots, which make up patterns of shapes and numbers visible to people with normal colour vision (Ishihara 1917). The second test was a Colour Arrangement Test (Farnsworth–Munsell 100 Hue Colour Vision test), which is used to observe differences perceived between colours by people with normal colour vision and those with colour vision deficits (Farnsworth 1943).

Study: An online password system was designed to collect password data. This type of system has been employed in a number of previous studies successfully (Woods 2017; Woods and Siponen 2018, 2019). The system allowed participants to create and recall passwords, and monitored correct input, and input errors. Over five weeks, five passwords per participant were created for five fictitious accounts. This design was employed to prevent cognitive overload, as learning many items at once, could have affected the recall results (Baddeley

Table 1. Demographic information.

Gender	Education level			
Male ($N = 41$; 46%)	Bachelor's degree ($N = 47$; 52%)			
Female ($N = 49$; 54%)	Master's degree ($N = 38$; 42%)			
	Doctoral degree ($N = 5$; 6%)			
Age distribution across groups				
Age range	Overall study ($N =$)	Control group (no colour) ($N =$)	Preselected colour group ($N =$)	Personally selected colour group ($N =$)
18–24 years	$N = 31$ (34.4%)	10	11	10
25–34 years	$N = 41$ (45.6%)	14	13	14
35–44 years	$N = 11$ (12.2%)	3	4	4
45–54 years	$N = 5$ (5.6%)	2	2	1
55–64 years	$N = 2$ (2.2%)	1	0	1

1992). To make the study as realistic as possible, the five account types varied in importance from online banking, to social networking, to online gaming. To increase the likelihood of participants engaging with the study, and treating the passwords as they were for real accounts; a technique was employed that has been used many times before with success: role-play (e.g. Forget, Chiasson, and Biddle 2008; Gaw and Felten 2006; Komanduri et al. 2011; Shay et al. 2010; Woods and Siponen 2018). The participants were asked to role-play, and imagine they were creating and recalling passwords for real accounts, even though they were aware they were fictitious.

Several previous studies have asked their participants to create passwords that meet common password policy rules (e.g. Shay et al. 2016; Woo et al. 2019; Woods and Siponen 2019); this study was no different. To create the five passwords to ensure a minimal level of strength and complexity, the participants were asked to create passwords that they were not using in their real-life, and that were at least eight characters long and contained characters including, uppercase and lowercase letters, digits and special characters. All passwords were dictionary checked, and were required to be unique from each other. As with previous studies (e.g. Shay et al. 2015; Woods 2017; Woods and Siponen 2018, 2019), feedback was provided to all participants when creating their passwords, on whether or how their passwords met the password rules, and when they did not. This allowed them to correct their errors and successfully create passwords while not decreasing strength. Along with the password rules, colour selection instructions were provided. The colour selection instructions were given to all groups, but differed for each group (see Table 2, for colour selection instructions). Colour selection instructions were given to the control group as well as the preselected colour group, to control for the action of selecting a colour on the cognitive processes and password recall results.

During the study, both objective and subjective data were collection. The objective data included all the

passwords recalled (correct and errors), and all the colour recalled (correct and errors). Subjective data were also collected by means of questionnaires that the participants completed after creating and recalling their passwords, and at the end of the study to enrich the data collection. The questionnaires were comprised of questions asking the participants about their experience with the study, including their techniques for creating and learning their passwords, their choice of colours and how colour effected their password memorability.

3.3. Stimuli

For the online password system, a grid of coloured and black squares was designed and presented to the participants (dependent on the group) when creating and recalling passwords. Once a square had been selected, then the participants would be able to create or recall their passwords in the corresponding colour.

The colours for the experiment were selected for several reasons: basic colour terms and names given to the colours; the interaction the colours had with the background of the interface; and the interaction the colour had with each other. The basic colour terms in English categories are: black, white, red, green, yellow, blue, brown, purple, pink, orange and grey. Even though conceptual differentiation between these colours could be conducted, not all the languages contain this categorisation (Berlin and Kay 1969). In addition to the basic colour terms, the colours were selected according to the colour terms that are the best remembered: red, orange, yellow, purple, green and white (Berlin and Kay 1969). The basic colour terms have gained criticism among scholars, for instance concerning the hierarchical categorisation of colour naming in cultures (e.g. Loreto, Mukherjee, and Tria 2012). Colour naming is difficult. People perceive colours differently and different meanings are attached to them across cultures, and therefore multiple colour names exist, which also implicates openness of language systems (e.g. Wyler 1992). For instance, describing green can vary from olive-green to grass-coloured. The reason why naming colours is important is that colours that have principal colour terms are remembered more easily than colours without principal terms (Biggam 2012). One reason why colour names enable enhanced memory performance is because colours with names create a mental concept of the colour in the mind (Biggam 2012). Enhanced memory performance also supports the selection of the basic colours (Berlin and Kay 1969) as the stimuli.

In this study, the colours were selected due to their noticeable difference from each other. This is because the user interface area in which the participants insert

Table 2. Colour selection instructions.

Control (non-colour) group	Preselected colour group	Personal selected colour group
'Please click on one of the boxes in the grid before creating a password'.	'Please click on the pre-selected colour from the menu before creating a password. Please remember the colour, as you will be asked to select it when recalling your password later'.	'Please choose a colour from the menu before creating a password. Please remember the colour, as you will be asked to select it when recalling your password later. You should select a different colour for each password created'.

the password and select the colour was white, which prevented the occurrences of unwanted colour contrasts, such as simultaneous contrast, in which complementary colours with same saturation and luminosity create optical illusions and change the appearance of the perceived colour (Itten 1973). Moreover, colours are constantly changing in relation to the surrounding colours. It is almost impossible to perceive a colour without the colour interacting with its surrounding colours (Albers 1975). Therefore, it has to be taken into account, when experimenting with colours, that the surrounding colours and the amount of colours in colour combinations influence the interaction of colours.

Overall, due to the selection criteria, the colours chosen were red, green, yellow, blue, brown, purple, pink, orange and grey (Table 3 presents the selected colours). Yellow colour was excluded from the colours due to its inefficient visual usability on a white background (Itten 1973). White colour was excluded because the background of the user interface in which the passwords are typed is white, which is also the case in most of the current user interfaces for the password typing area. However, because conventionally passwords are typed in black, this colour was used for the control group. Moreover, to increase the amount of the colours for participants in the experimental groups, a dark and light version of the colours were included. This addition was also in line with Berlin and Kay's basic colour terms (1969), in which dark (black) and bright (white) colour terms are also included, because all cultures have terms for these. Furthermore, only one colour was allowed to be selected at once and was displayed with a white background. This was crucial as not to enable the colours to interact with each other, and to change the perceived colour.

3.4. Procedure

Ethical considerations were taken into account. Extensive information about the study was provided to all participants before asking for their consent. Consent was asked for participation and for allowing the collected data to be used in scientific research. The

participants were informed that the information they provided would be anonymised, and kept confidential. Furthermore, the participants were given the right to withdraw at any point.

A recruitment advertisement was posted on the university's website, and sent out across the university's emailing lists to recruit participants. A weblink was supplied within the advert that took participants to the website where they could find about the study and sign up. The participants were given information about the study, including what to expect over the five weeks. They were informed about how they would be contacted, what level of involvement would be required, and that they would be creating and recalling passwords for fictitious accounts, and completing questionnaires about their experience. This information was also made available throughout the study. Participants who agreed to take part in the study gave their formal consent and were informed at the beginning and throughout the study that they had the right to withdraw at any point. As a part of the recruitment stage, all those wanting to take part in the study undertook two colour blindness tests. Those who were considered colour-blind, were exempt from the study. The rest of the participants were allowed into the three groups.

The participants from all three groups completed the same study. The longitudinal experiment was conducted 1–2 times per week during five weeks. When the participants were required to interact with the study, an email was sent giving instructions on what was required. The passwords were created, learnt, and recalled several times during the five weeks. One password was created in week 1, and in weeks 2 and 3, two passwords were created. Two passwords were recalled every week, (apart from week 1, when one password was recalled, and in week 5, when five passwords were recalled). The study schedule is presented in Table 4.

The groups were defined by the presence of colour, and if the colour was preselected by the experimenters or personally chosen by the participants. The colours that were preselected by the experimenters are shown in Table 5.

Table 3. The colours used in the experiment with Hex codes.



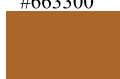

Red	Green	Blue	Brown	Purple	Pink	Orange	Grey
							
Dark #A50021	Dark #006400	Dark #17365D	Dark #663300	Dark #8B0080	Dark #DB006E	Dark #E36C0A	Dark #595959
							
Light #FF1515	Light #76923C	Light #548DD4	Light #996633	Light #CA5E94	Light #FF42C0	Light #F4AB62	Light #7F7F7F

Table 4. Password creation and recall schedule.

Week	Number of passwords created	Number of passwords recalled	Which password: Account type
1 beginning	1	1	Online Banking
1 end			Online Banking
2 beginning	2	2	Email/Social Networking
2 end			Online Banking/Email
3 beginning	2	2	Online Shopping/Online Gaming
3 end			Online Shopping/Online Gaming
4 beginning		2	Social Networking/Online Shopping
4 end			
5 beginning		5	All
5 end			

Table 5. Preselected colours and allocated account types.

Account type	Online banking	Email	Social Networking	Online Shopping	Online Gaming
Preselected color	Dark Green *****	Light Purple *****	Dark Red *****	Light Grey *****	Dark Orange *****

When creating or recalling passwords, all participants were presented with a grid of coloured or black squares (an example screenshot is presented in Figure 1).

The personal selected colour group were asked to select a colour by clicking on only one of the 16 colours from the grid before creating or recalling their passwords. When they started to type into the box provided, the passwords would be presented in the corresponding colours. To make the password creation process consistent across groups, the participants in preselected colour group were presented with the same grid of 16 colours (as with the personal selected colour group) and were asked to click on the colour before they could type in their password, even though the colour was preselected by the experimenter. For both experimental groups, when recalling

their passwords, the participants were asked to recall which colour was saved with the password, and to click on the colour before they could enter the password. Again, when the participants started to type into the box provided, the passwords would be presented in the corresponding colours (presented in Figure 2). The password system was designed to change the position of the colours within the grid every time the participants created and recalled their passwords. This was with the purpose of controlling for the effect of remembering the position of the colour rather than the colour itself. The control group were also presented with a grid, but this time with black squares to make the creation and recalling password process consistent with the other groups. They were asked to select any black square from the grid before typing in their

Study About Instructions Logout Withdraw

Please choose a color from the menu before creating a password. Please remember the color, as you will be asked to select it when recalling your password later. You should select a different color for each password created

Online bank

Create password

Enter password

Submit

Guidelines for creating passwords

Each password must:

1. contain at least eight characters.
2. contain at least one number (0-9).
3. contain at least one lower case letter (a-z).
4. contain at least one upper case letter (A-Z).
5. contain at least one special character (e.g. !, %, &).
6. to contain no words or names (e.g., J78sk7la3?).
7. be unique = different from every other password created, preferably different in meaning too (e.g., J78sk7la3? and ilo>TK1!).

*** AT NO POINT SHOULD YOU WRITE ANY PASSWORDS DOWN***

Accounts:

- Online Banking - online banking account
- Email - email account
- Social Networking - social networking account
- Online Shopping - online shopping account
- Online Gaming - free online gaming account

Figure 1. Example screenshot of the password creation page for the personal selected colour group.

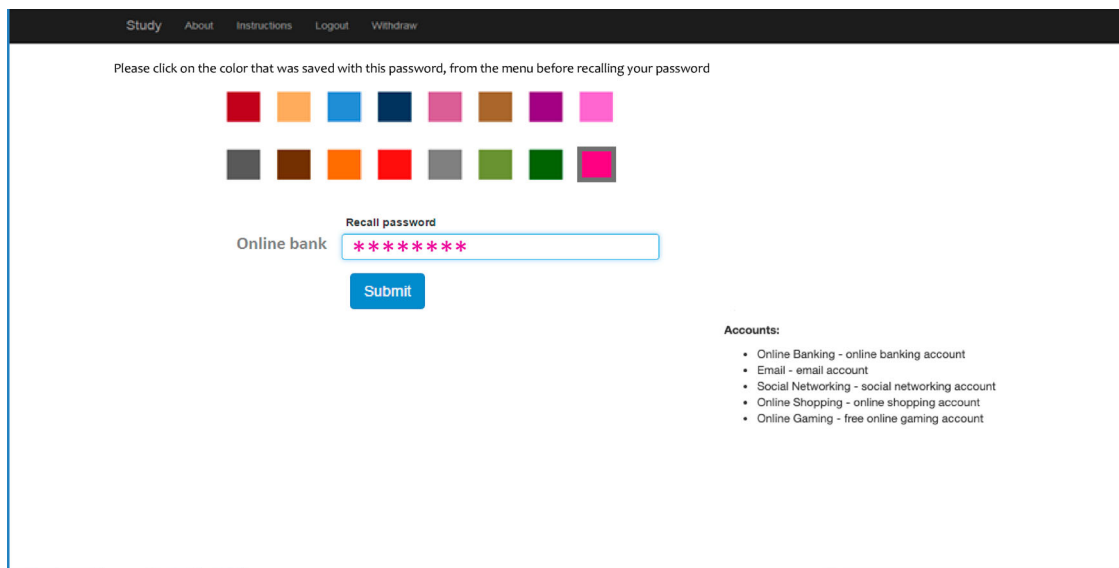


Figure 2. Example screenshot of the password recall page for the preselected and personal selected colour groups.

passwords when both creating and recalling their passwords. The passwords would appear in black. All participants in all three groups were given three attempts to recall their passwords correctly, and if they did not then the system would move on to the questionnaire.

After creating and recalling their passwords (regardless if they correctly recalled their passwords), the participants in all three groups were asked to complete online questionnaires to report on their experience with the study, and answer questions regarding their choice of colour (personal selected colour group only).

The participants were sent an email when they had completed each part of the study and reminders if they had not taken part. They were sent confirmation emails of when they had finally completed the whole study with details of the study and how to collect their movie tickets.

4. Results

A large amount of data was analysed from 90 participants, collected by means of an online password system, specifically designed for this study. Each participant created five passwords, and recalled them 12 times, with up to 3 attempts each time. Therefore, over 3000 passwords were collected over the five weeks when participants created and recalled their passwords. Colour choices were also collected with the passwords from the personal selected colour group, and colours recalled by both experimental groups. Subjective data in the form of questionnaire responses reporting on colour choices and study experience were also collected. To test the hypotheses, between-subjects analysis of variance (ANOVA) tests were used to confirm the differences between the two experimental and control groups.

4.1. Correct password recall

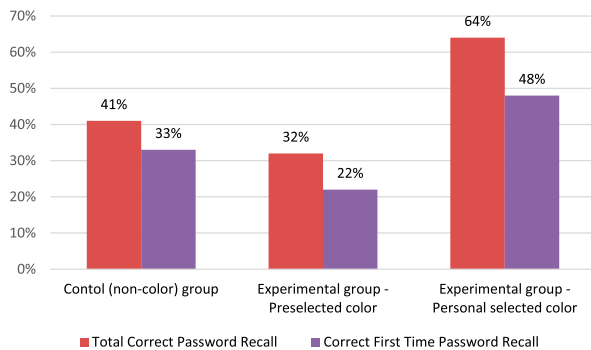
Correct password recall was classified into the number of times passwords were correctly recalled on the first attempt (correct first time password recall), and the total number of passwords correctly recalled (total correct password recall). For a password to be considered successfully or correctly recalled, the colour would need to match the one selected for the specific password, and the password content to be correct also. Between-subjects ANOVA were employed to examine the effect of colour on password recall. There was a significant difference between the groups for correct first time password recall ($\chi^2 = 14.722$, $df = 2$, $p = 0.001$) and total correct password recall ($F_{(2,87)} = 11.578$, $p < 0.001$). However, the lowest mean scores of correct password recall (correct first time and total correct password recall) (see Table 6) were found in the preselected colour group compared with both the control (non-colour) group and the personal selected colour group, not supporting H1 (see Table 7). The success rates for both total correct password recall and correct first time password recall are represented in Figure 3.

Table 6. Descriptive statistics.

Mean, standard deviation and range	Control (non-colour) group (N = 30)	Preselected colour group (N = 30)	Personal selected colour group (N = 30)
Password recall:			
Total correct password recall	4.93 (3.36) (0–12)	3.87 (3.05) (0–12)	7.67 (3.04) (0–12)
Correct first time password recall	4.00 (3.09) (0–12)	2.63 (2.71) (0–12)	5.77 (3.19) (0–12)
Colour memorability	N/A	5.77 (3.04) (0–12)	8.80 (2.54) (0–12)

Table 7. Inferential statistics.

Variables	Hypotheses	Supported/Sig.
Password recall Colour	H1: Coloured passwords will have a positive effect on correct password recall, compared with passwords with no colour.	$\chi^2 = 14.722$, $df = 2$, $p = 0.001$ (correct first time password recall) $F_{(2,87)} = 11.578$, $p < 0.001$ (total correct password recall) Overall, not supported
Colour memorability Colour: Personal selected/ Preselected	H2: Personally selected colours will have a positive effect on memorability of colours than preselected colours.	$U = 206.000$, $N_1 = 30$, $N_2 = 30$, $p < 0.001$, one-tailed Supported
Password recall Colour: Personal selected/ Preselected	H3: Personally selected colours will have a greater positive effect on correct password recall, compared with passwords with preselected colour and passwords with no colour.	Personal selected colour \times Preselected colour ($p < 0.001$) Personal selected colour \times No colour ($p = 0.004$) Preselected colour \times No colour ($p = 0.58$) Overall, supported

**Figure 3.** Success rates of password recall.

4.2. Colour memorability

Colour memorability was measured as the number of times the colour was recalled correctly, irrespectively of if the password was correctly recalled. In the preselected colour group, for each password created the participants were given a colour and asked to learn it with the password they created, and were then asked to recall the password and corresponding colour. In the personal selection colour group, participants were asked to choose a colour and learn it with the password they created, and then to recall both colour and password. A

Mann–Whitney U test (non-parametric t -test, due to data distribution) was performed to analyse the difference between the preselected and personally selected colour groups to see whether choosing or having a colour chosen would have an effect on the memorability of the colour. We found that colour memorability was significantly higher in the personal selection colour group compared with the preselected colour group ($U = 206.000$, $N_1 = 30$, $N_2 = 30$, $p < 0.001$, one-tailed), supporting H2. Descriptive and inferential statistics are shown in Table 6 and 7.

4.3. Personal selection of colour and password memorability

From the between-subjects ANOVA test that was employed to examine the effect of colour on total correct password recall, *post hoc* pair-wise comparisons with Bonferroni correction showed there was no significant difference between the preselected colour group and the control group ($p = 0.58$). However, it did show that total correct password recall was significantly higher in the personal selected colour group, compared with the control (non-colour) group ($p = 0.004$), and compared with preselected colour group ($p < 0.001$), supporting H3 (see Table 6 and 7).

4.4. Further analysis

During the study, a considerable amount of data was collected measuring password recall, colour memorability, and colour preferences. Further analysis was conducted to give a more enriched understanding of how colour affects password memorability.

4.4.1. Colour memorability

Through analysing the data, we found that colours were more successfully remembered when the participants chose the colour, compared to when it was preselected. To support our results, we looked deeper into which colours were more memorable to see if they had an effect (represented in Table 8).

The preselected colour group had the lowest level of successful password recall out of the three groups and the lowest colour memorability out of the two

Table 8. Preselected colours and percentages of correct recall.

Account type	Preselected color	Color most successfully recalled	Percentage of correct recall
Online banking	Dark Green	Dark Green	38.3%
Email	Light Purple	Light Grey	28.3%
Social Networking	Dark Red	Dark Orange	11.7%
Online Shopping	Light Grey	Dark Red	11.7%
Online Gaming	Dark Orange	Light Purple	10.0%

experimental groups. However, out of the preselected colours dark green and light grey were the most memorable. Dark green was the first colour to be learnt; however, light grey was not the second colour to be learnt nor the last, which could have suggested a primacy and recency effect (Baddeley and Hitch 1977). Nevertheless, out of the five accounts the online banking and the online shopping account, i.e. the accounts for which these colours were assigned, were recalled more often than the other three accounts (three times, instead of two times), this may suggest why they were more highly recalled.

The personal selected colour group was able to choose between 16 different colours. The colours chosen are reported in Table 9 in rank order of choice. The recall rate showed to be different to the colours that were preferred (shown in Table 9). Dark blue was not the most chosen colour, but was still very popular (ranked 3rd). It was most used for the online banking; although, it was used only once for the online shopping account. Overall, it was the highest recalled colour. Light red was also very popular (ranked 2nd), especially for online banking and shopping, however, it was used only once for the social networking account, and was not used for online gaming. It had the second highest recall rate; this could be a result of these accounts being recalled three times compared with two times for the other accounts. Light grey was of average popularity (ranked 7th), it was not used for the online banking nor email accounts, however, it ranked third for memorability. Dark orange was above average in popularity, its use was distributed across all accounts, and was ranked fourth in memorability. Light blue was more popular, but was mainly used for email and social networking. Dark green, on the other hand was the most

chosen of colours, but was ranked sixth in memorability. It was used fairly equally across all accounts, however, it was not used at all for the online gaming account.

Are the colours comparable in terms of memorability? Dark red and light purple were harder to remember for both preselected colour group and personal selected colour group. Dark green, even though it was the most chosen of colours in the personal selected colour group, it was not as memorable as some other colours. In the preselected colour group, it was the most remembered colour, however, this could be due to the number of times it was required to be recalled. Light grey and dark orange were better remembered than most colours across both groups (Table 10 compares the two colour memorability rankings). From these results, it is hard to infer that the colours were comparable between groups, suggesting that just the colours (without any personal meaning), would be memorable enough on their own. However, during the study all participants completed several questionnaires, after creating and recalling passwords, and at the end of the study for a more in-depth account of the meaning that the participants associated with the colours and their effect on their memorability.

4.4.2. Colour and account

The participants in the experimental groups were asked how strongly they thought the colours were related or associated with the accounts, and why. The majority of participants in the preselected colour group found that the colours were not related to the accounts. Only a few participants reported that the colour was strongly related or related to the accounts due to them personally finding an association to help them remember (see Figure 4).

Table 9. Personal selected colours, and ranking of correct recall with percentages.

Selected colors	Percentage of selection	Most successfully recalled color (increase, decreased, or remained the same place in rank as selected color order)	Percentage of correct recall
Dark Green	12.8%	Dark Blue (+ 2)	14.4%
Light Red	12.0%	Light Red (=)	13.0%
Dark Blue	11.2%	Light Grey (+ 4)	10.3%
Light Blue	8.8%	Dark Orange (+ 1)	9.6%
Dark Orange	7.2%	Light Blue (- 1)	9.6%
Dark Purple	7.2%	Dark Green (- 5)	8.2%
Light Grey	7.2%	Dark Purple (- 1)	6.9%
Light Pink	7.2%	Light Pink (=)	6.2%
Dark Grey	5.6%	Dark Grey (=)	4.8%
Dark Pink	5.6%	Light Green (+ 1)	4.8%
Light Green	4.0%	Light Purple (+ 2)	4.8%
Dark Brown	3.2%	Dark Pink (- 2)	2.7%
Light Purple	3.2%	Dark Brown (- 1)	2.1%
Light Orange	2.4%	Light Orange (=)	1.4%
Dark Red	1.6%	Dark Red (=)	0.7%
Light Brown	0.8%	Light Brown (=)	0.8%

Table 10. Comparison of rank order of preselected and personally selected colours most successfully recalled.

Rank order of preselected colors most successfully recalled	Rank order of personally selected colors most successfully recalled
Dark Green	Dark Blue
Light Grey	Light Red
Dark Orange	Light Grey
Dark Red	Dark Orange
Light Purple	Light Blue
	Dark Green
	Dark Purple
	Light Pink
	Dark Grey
	Light Green
	Light Purple
	Dark Pink
	Dark Brown
	Light Orange
	Dark Red
	Light Brown

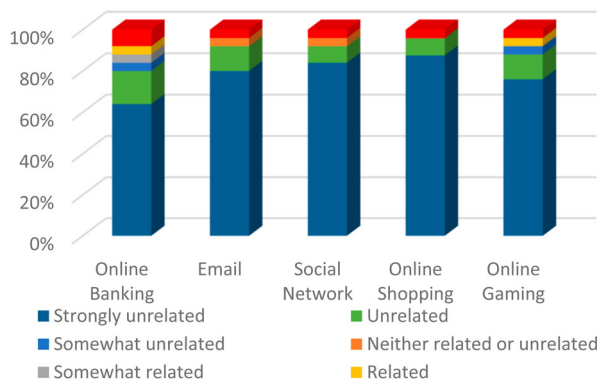


Figure 4. How strongly the colours were thought to be related to the accounts in the preselected colour group.

The participants in the personal selected colour group found more association with the accounts, this was due to them being able to select the colour themselves and attach their own meaning for the association (see Figures 5–7).

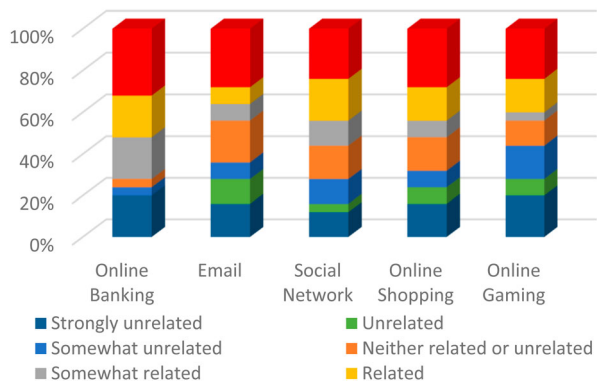


Figure 5. How strongly the colours were thought to be related to the accounts in the personal selected colour group.

4.4.3. Colour and password memorability and security

The participants were asked if the choice of colour helped them remember their passwords, and if so, how it helped. Fifty-one percent of the selected colour group reported that the colours helped them remember their passwords, compared to 15% from the preselected colour group. Out of the 51% in the selected colour group, the participants’ responses referred to the colours helping them remember the accounts (e.g. the colour of the logo, from their own personal account), or it helped them remember something related to the service of the accounts (e.g. money for online banking). The participants also referred to the colours being associated with the content of the passwords (e.g. the colour was included in the password in some form), or the colours helped them form and create the passwords. Other responses referred to the colours having personal meaning for them. For the preselected colour group all responses for how the colours helped them remember their passwords, referred to the content of the password or how they were formed. There were no responses suggesting that the colours were related to the accounts or could help them remember the accounts (see Figure 6).

When examining the responses to how the participants created their passwords, there was a notable difference between the groups in terms of their reasoning for choosing their passwords. The control (non-colour) group had a higher number of reported chosen passwords because they were easy to remember, compared with using a memory technique, rules or patterns; even the using the accounts to help them create and learn their passwords. The preselected colour group also reported higher numbers of choosing passwords due to them being easy to remember. However, they

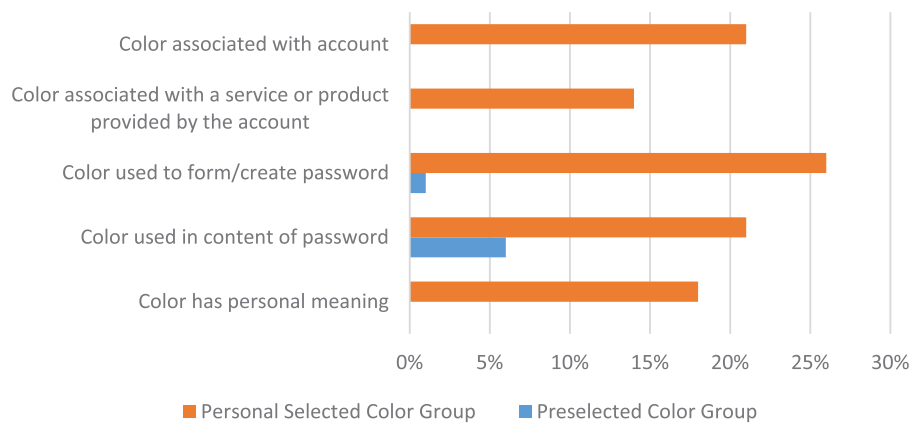


Figure 6. Participants' responses: reasoning for why colour helped password memorability.

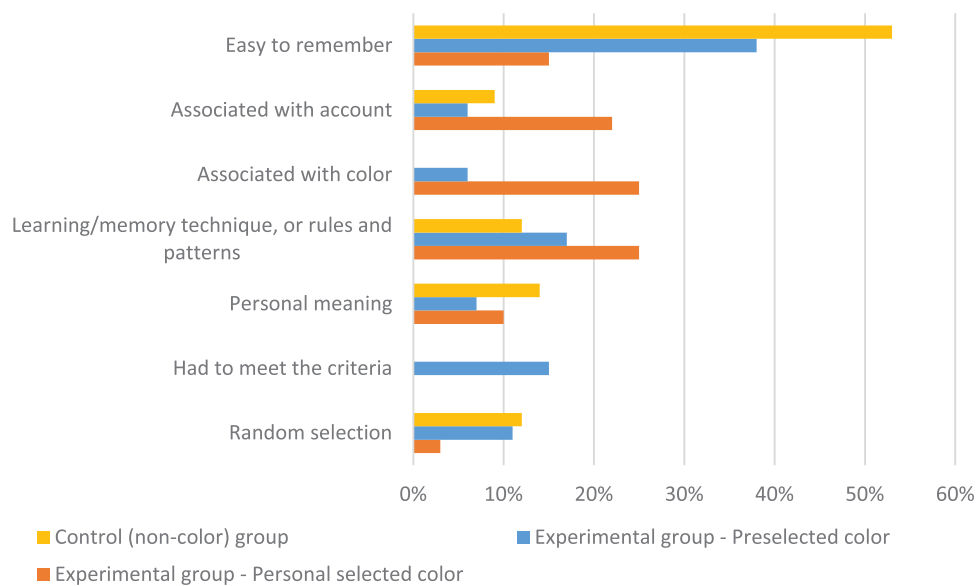


Figure 7. Participants' responses: reasoning for why they chose their passwords.

had slightly higher numbers of using memory techniques, but using the colour to help them create their passwords was low (6%), and so too, using the accounts (6%). They did however, have a response not found in the other groups; 15% reported that they chose their passwords just to meet the criteria of the password rules. The personal selected colour group reported higher numbers of passwords being created with memory techniques, associating them with accounts and the colours they chose, and there were less passwords being chosen just because they were easy to remember, and less being chosen randomly compared to the other two groups. These results suggest that the presence of colour, and more importantly being able to choose colour encouraged the participants to add more meaning and effort to creating passwords and learning them.

Nonetheless, this does raise the question about security; through the use of colour, could the security of the passwords be compromised by incorporating the colour into the content of the password? This could potentially occur if the user uses this type of insecure behaviour. Although, within our study, out of the two colour groups ($N = 60$) with each participant creating 5 passwords each (totalling 300 passwords), only 11 passwords showed to have an 'obvious' incorporation of colour in the content of the passwords. For example, 'Purpl3-viole#' (colour: dark purple), '0R45t%e21' (colour: dark orange) and 'H4rm44781!' (colour: light grey (Harmaa in Finnish)). Participants reported to use colour in the content of their passwords (see Figure 6), however, those who did, created random passwords that were difficult to see any connection with the colour.

5. Discussion

The security of password authentication is a pertinent issue as users often chose memorability over security (Grawemeyer and Johnson 2011; Tam, Glassman, and Vandenwauver 2010; Weir et al., 2009; Zhang et al. 2009). The trade-off between password security and memorability leads to many security breaches that result in financial losses and privacy threats to organisations and home-users (Brostoff and Sasse 2000; Brown et al. 2004; Hayashi et al. 2012; Saastamoinen 2014; Vu et al. 2007). The purpose of this study is to tackle this issue by suggesting the incorporation of colour into the password process, employing it as a memory cue and as an additional security parameter. Based on our results we will next discuss our findings, and the implications of our findings.

5.1. Colour and password memorability

Colour has been used previously within security research adding an additional security parameter to graphical passwords, and to PIN codes (Biddle, 2012; Chiang and Chiasson 2013; Khamis et al. 2019; Renaud and Ramsey, 2014; Thoopsamut and Limthanmaphon 2019; van Oorschot and Thorpe 2008). However, as of yet, it had not been added to text-based passwords within the font of the password. The results have important implications, as where colour has been found to improve password memorability; it has only shown improvements when it has been chosen by the user. Testing this small distinction has shown significant results, showing that including colour (personally selected) into the creation and recalling password process, could increase password memorability by 21%, compared with current practices (using black font). However, it is also important to understand why choosing the colour was essential to password memorability.

5.2. Colour memorability

Another important finding from this study was that personal selection of colours positively affected the memorability of colours when compared with colours that were preselected. After examining the highest and lowest ranking recalled colours, we found that the colour alone (it just being present in the environment) was not enough to effect memory performance, and therefore, not supporting encoding specificity principle (Tulving and Thomson 1973). The theory would suggest that the colour just being present when creating the passwords and then when recalling them would

improve memory performance; ‘evidence suggests that colour should aid memory performance only when items are identically coloured at study and test’ (Hanna and Remington 1996, 323). However, when Hanna and Remington were examining encoding specificity principle and visual stimuli, such as colour, they were pairing the colours with geometric shapes as their visual stimuli, which would be cognitively processed differently to the written word, or in this instance a complex random text-based password. After examining the participants’ responses, we found that the preselected colour group reported the colours were strongly unrelated to the accounts. However, there were a small number of participants who thought the opposite, but reported that they had made an effort to find a connection and meaning between the preselected colours and accounts, to aid them in their password memorability. This finding supports findings by Hanna and Loftus (1993), that colour needs more than perceptual processing to be encoded properly, conceptual processing is required and having a strong relationship with the item to be remembered.

5.3. Personal selection of colour and password memorability

Personal selection of colours had a significantly greater effect on password recall (63%) than current practices (black font) (42%) or having the colours preselected (34%). The differences between being able to personally select the colours and having them preselected are consistent with findings from Renaud and Ramsey (2014), where preselected colours were used to aid PIN memorability. They found that the colours did not improve PIN memorability, and concluded that this was due to the lack of meaningful associations between the colours and numbers.

In the current study, we found that 15% of the preselected colour group reported that colour helped with recalling their passwords, as they were used as a memory cue in creating the passwords or relating them to something within the passwords. Colour affects memory if used as a cue; presence alone is not enough (Hanna and Loftus 1993). Therefore, 6% of the preselected colour group used the colour as a memory cue when creating their passwords, and 15% found it helped them recall their passwords. Consequently, the remaining participants in the group, had to learn and recall the preselected colour in addition to their passwords, which would increase cognitive load (more to remember); these results are consistent with findings from Renaud and Ramsey (2014).

The personal colour selection group used their choice of colours in a more varied way in creating, learning and recalling their passwords. They reported that the colours helped them recall their passwords by helping them think of the accounts, passwords and through adding meaning. These results are supported by Palmer and Schloss (2010), associating colour with objects, as for example, online banking websites often use blue; and within the study, participants selected colours that were associated with the accounts (e.g. logo). Moreover, in the creation stage, more participants in the personal colour selection group reported to create their passwords with memory techniques, using the colour and accounts as memory cues, and created less ‘random’ (less meaningful) passwords than the other two groups. Therefore, the colours were not additional items to be learnt, but a means to elicit the target items – the passwords. The option of choosing colours encouraged the participants in the group to create more personal and meaningful memory cues to aid their password memorability.

5.4. Personal selection of colour and password security

Within the study, a minimum level of strength was imposed through the password creation rules. All passwords were of a minimum length (min. eight characters long), complexity (including upper and lower letters, numbers and special characters), no names or words were allowed, therefore, the passwords were random, and finally, all passwords had to be unique from each other (max. three characters in common). Through imposing these password creation requirements, we had imposed a minimum level of strength; however, additional strength came from two perspectives. Firstly, choosing colours as a part of the passwords adds another parameter increasing all passwords’ entropy (Biddle, 2012; van Oorschot and Thorpe 2008). Secondly, by creating more meaningful memory cues with their passwords, users will increase their password memorability that will lead to less insecure password behaviours being adopted, for example, password reuse. Furthermore, choosing colours would be effective in terms of password security as cultural relativity of colour preferences (Taylor, Clifford, and Franklin 2013) would increase the variability of colour selection in the password process.

5.5. Implications for practice

Previous research highlights the trade-off between password memorability and password security; if one factor

(password memorability) increases then another (password security) decreases (Brown et al. 2004; Hayashi et al. 2012; Vu et al. 2007; Woods and Siponen 2018). Our insightful study had some important results that suggest this does not necessarily have to be the case, and furthermore uncovered some significant findings that bring a better understanding of how colour can be used as a memory cue, and how it can improve password memorability and security simultaneously.

Renaud and Ramsey (2014) in their paper, warned manufacturers to be careful using colours for ATM machines, as the additional preselected colours could decrease the memorability of PINs. However, in our study, the experimental colour groups were divided into preselected colours and personally selected colours, revealing that colour can improve memorability if it is chosen and a meaningful association is formed. Therefore, the implications of our results affect organisations and home-users, through the incorporation of a selection of colours into the password requirements, and where the user can choose the colour; not only can this increase password memorability, but it can also increase password security. With increased password memorability, users will be struggling less with their passwords, which will result in a reduction of insecure password behaviours (such as writing passwords down, modifying and reusing passwords) being adopted by users (Adams and Sasse 1999; Campbell, Kleeman, and Ma 2006; Inglesant and Sasse 2010; Marquardson 2012; Zhang et al. 2009). Moreover, with less insecure passwords behaviours being adopted, and that colour passwords would be more secure with the extra security parameter, this will both reduce security breaches and the consequences that arise from them (Das et al. 2014; Hayashi et al. 2012; Saastamoinen 2014; Vu et al. 2007).

5.6. Study limitations

5.6.1. Ecological validity

When examining the human memory, employing a laboratory design is often a preferred means of data collection to ensure precision and control over the variables (Dennis and Valacich 2001; Liu and Myers 2011). Many previous password memorability studies employ such designs (e.g. Fahl et al. 2013; Nelson and Vu 2010; Vu et al. 2007; Wiedenbeck et al. 2005; Woods and Siponen 2018, 2019; Zhang et al. 2009). However, it has to be acknowledged that while a design such as this brings precision of data, it also brings some drawbacks pertaining to realism. To counter the realism issue, the study was designed in such a way to be as realistic as possible: the participants created and recalled their passwords online, and over a period of time (not

just all at once). Previous studies have brought to light that password studies that are online are more representative of participants' actual password behaviour (Fahl et al. 2013; Shay et al. 2016). However, within the study, the participants were aware they were creating and recalling passwords for fictitious accounts, which could have potentially affected their motivation to learn and recall their passwords. Therefore, the participants were asked to role-play, a technique used in many previous studies (e.g. Forget, Chiasson, and Biddle 2008; Gaw and Felton, 2006; Komanduri et al. 2011; Shay et al. 2010, 2015, 2016; Woo et al. 2019). It was stipulated before the study began, 'We would appreciate it if you would learn your passwords to the best of your ability, and consider them as protecting "real" accounts, as we will monitor your interaction with the system'. Previous studies have found that role-playing in password creation and recall studies, helps the participants create stronger passwords, helps them engage more with the experiment, and helps the participants treat the passwords as genuine (Komanduri et al. 2011; Shay et al. 2015, 2016; Woo et al. 2019).

5.6.2. Writing password down

By increasing the realism of the study, where the participants created and recalled their passwords online, could potentially allow the participants to write their password down. However, throughout the study participants were asked and reminded not to do so, suggesting that they would be breaking the rules and such behaviour could lead to security breaches. Furthermore, at the end of the study participants were asked, 'During this study, did you use any memory aids, techniques or strategies to help remember your passwords?' and were given the options of 'Yes/No, if yes ... wrote it down, saved it electronically, used a memory technique to remember, or other ...'. Only one participant had reported to have written one of their passwords down (from the preselected colour group), but they reported that they did not record the colour, and subsequently forgot it. For the other passwords, they used a memory technique to learn and recall them. Overall, several of participants reported that they had used memory techniques to help them recall their passwords, with only that one instance of writing down one password but forgetting the colour.

5.7. Future research

This study revealed some interesting findings; however, future research could extend the longitudinal study design for a longer period of time, to see whether the improved password memorability is consistent for a

longer period of time. Other suggestions for future research could involve increasing the number of passwords to be learnt and recalled, and different variations of accounts. Future research could also examine if more colours could be included into the design, and whether too many colours would increase password and colour interference. Other suggestions for future research could include examining other visual elements that could be incorporated in the same way as colour was in this study, such as style of font, which would increase password memorability and security concurrently.

5.8. Conclusion

Password security is imperative in this digital age. However, users are compromising the authentication mechanism due to the large number of passwords they have to remember (Grawemeyer and Johnson 2011; Zhang et al. 2009). As the number of passwords increases due to the number of online accounts increasing, the ability of users to cope with remembering multiple passwords diminishes. Therefore, many users will adopt insecure password behaviours to cope with their limitations (Biddle, Chiasson, and Van Orschot 2012; Duggan, Johnson, and Grawemeyer 2012; Gaw and Felton 2006; Grawemeyer and Johnson 2011; Notoatmodjo and Thomborson 2009; Stobert and Biddle, 2018; Zhang et al. 2009). This is resulting in a trade-off between password memorability and security, and therefore, finding new ways in which to increase both factors simultaneously is of the utmost importance. In this study, colour was examined to see whether it could be utilised as a memory cue to improve password memorability and security.

Over 3000 passwords were created, learnt and recalled (password process) over a five-week period in a longitudinal study. Objective (colour and password recall) data and subjective (participant questionnaire responses on colour and password recall) data, led to a plethora of enriched results, and interesting findings. The results suggest that by adding colour to the password process, password memorability can be increased by over 20% when compared with current practices (black font). Choosing colours (compared with colours being preselected), encouraged participants to create more meaningful memory cues to help them increase their password memorability. Moreover, adding colour provided another security parameter, increasing password entropy. These results have significant implications for organisations and home-users, as increasing password memorability and security at the same time, could lead to a reduction in security

breaches, and therefore, a reduction in the financial losses suffered due to password security breaches.

Acknowledgements

The authors would like to thank the participants for taking part in the long study.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

- Adams, A., and M. Sasse. 1999. "Users Are Not the Enemy." *Communications of the ACM* 42 (12): 41–46.
- Al-Ameen, M. N., S. T. Marne, K. Fatema, M. Wright, and S. Scielzo. 2020. "On Improving the Memorability of System-assigned Recognition-based Passwords." *Behaviour & Information Technology* 41 (5): 1115–1131.
- Al-Ameen, M. N., M. Wright, and S. Scielzo. 2015. "Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues." Proceedings of the Enhanced Security with Passwords & CAPTCHAs, CHI '15, Seoul, Republic of Korea, 2315–2324.
- Albers, J. 1975. *Interaction of Color: Text of the Original Edition with Revised Plate Section*. New Haven, CT: Yale University Press.
- Alkaldi, N., K. Renaud, and L. Mackenzie. 2018. "Encouraging Password Manager Adoption by Meeting Adopter Self-Determination Needs." Proceedings of the 52nd Hawaii International Conference on System Sciences, HICSS, Hawaii.
- Anderson, M. 2009. "Incidental Forgetting." In *Memory*, edited by A. D. Baddeley, M. W. Eysenck, and M. C. Anderson, 191–216. Hove & New York, NY: Psychology Press.
- Atkinson, R. C., and R. M. Shiffrin. 1968. "Human Memory: A Proposed System and Its Control Processes." *Psychology of Learning and Motivation* 2: 89–195.
- Baddeley, A. D. 1992. "Working Memory." *Science* 255: 556–559.
- Baddeley, A. D. 2009a. "What is Memory?" In *Memory*, edited by A. D. Baddeley, M. W. Eysenck, and M. C. Anderson, 1–18. Hove & New York, NY: Psychology Press.
- Baddeley, A. D. 2009b. "Memory and Aging." In *Memory*, edited by A. D. Baddeley, M. W. Eysenck, and M. C. Anderson, 293–316. Hove & New York, NY: Psychology Press.
- Baddeley, A., and G. J. Hitch. 1974. "Working Memory." In *Recent Advances in Learning and Motivation*, edited by G. A. Bower, 8, 47–89. New York: Academic Press.
- Baddeley, A., and G. J. Hitch. 1977. *Recency re-Examined, Attention and Performance VI*. Hillsdale, NJ: Lawrence Erlbaum Associates, pp. 647–667.
- Bang, Y., D. Lee, Y. Bae, and J. Ahn. 2012. "Improving Information Security Management: An Analysis of ID-Password Usage and a New Login Vulnerability Measure." *International Journal of Information Management* 32: 409–418. doi:10.1016/j.ijinfomgt.2012.01.001.
- Berlin, B., and P. Kay. 1969. *Basic Color Terms: Their Universality and Evolution*. Berkeley: University of California.
- Biddle, R., S. Chiasson, and P. C. Van Orschot. 2012. "Graphical Passwords: Learning from the First Twelve Years." *ACM Computing Surveys* 44 (4): 19:11–19:41. doi:10.1145/2333112.2333114.
- Biggam, C. P. 2012. *The Semantics of Colour: A Historical Approach*. Cambridge: Cambridge University Press.
- Bonneau, J., and S. Preibusch. 2010. "The Password Thicket: Technical and Markey Failures in Human Authentication on the Web." Proceedings of the 9th Workshop on the Economics of Information Security, WEIS 2010, Boston, MA, 1–49.
- Brostoff, S., and M. A. Sasse. 2000. "Are Passfaces More Usable Than Passwords? A Field Trial Investigation." Proceedings of the HCI2000: People and Computers XIV – Usability or Else. Springer, Sunderland, UK, 405–424. doi:10.1007/978-1-4471-0515-2_27.
- Brown, A. S., E. Bracken, S. Zoccoli, and K. Douglas. 2004. "Generating and Remembering Passwords." *Applied Cognitive Psychology* 18 (6): 641–651.
- Campbell, J., D. Kleeman, and W. Ma. 2006. "Password Composition Policy: Does Enforcement Lead to Better Password Choices?" Proceedings of the 17th Australasian Conference on Information Systems Password Composition Policy, ACIS, Adelaide, Australia, 60.
- Chiang, H. Y., and S. Chiasson. 2013. "Improving User Authentication on Mobile Devices: A Touchscreen Graphical Password." Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services, 251–260.
- Chiasson, S., P. C. van Oorschot, and R. Biddle. 2006. "A Usability Study and Critique of Two Password Managers." The Proceedings of the 15th USENIX Security Symposium '06, 1–16.
- Cohen, J. 1992. "A Power Primer." *Psychological Bulletin* 112 (1): 155–159.
- Craik, F., and R. Lockhart. 1972. "Levels of Processing. A Framework for Memory Research." *Journal of Verbal Learning and Verbal Behavior* 11: 671–684.
- Das, A., J. Bonneau, M. Caesar, N. Borisov, and X. Wang. 2014. "The Tangled Web of Password Reuse." Proceeding of NDSS'14, San Diego, CA, 23–26.
- Dennis, A., and J. Valacich. 2001. "Conducting Research in Information Systems." *Communications of the AIS* 7 (5): 1–41.
- Derefeldt, G., T. Swartling, U. Berggrund, and P. Bodrogi. 2004. "Cognitive Color. Color Research & Application: Endorsed by Inter-Society Color Council, The Colour Group (Great Britain), Canadian Society for Color, Color Science Association of Japan, Dutch Society for the Study of Color, The Swedish Colour Centre Foundation, Colour Society of Australia." *Centre Français de la Couleur* 29 (1): 7–19.
- Duggan, G. B., H. Johnson, and B. Grawemeyer. 2012. "Rational Security: Modelling Everyday Password Use." *International Journal of Human-Computer Studies* 70: 415–431. doi:10.1016/j.ijhcs.2012.02.008.
- Fahl, S., M. Harbach, Y. Acar, and M. Smith. 2013. "On the Ecological Validity of a Password Study." Proceedings of the ninth Symposium on Usable Privacy and Security (June 201), 1–13.

- Farley, F. H., and A. P. Grant. 1976. "Arousal and Cognition: Memory for Color Versus Black and White Multimedia Presentation." *The Journal of Psychology: Interdisciplinary and Applied* 94 (1): 147–150.
- Farnsworth, D. 1943. "The Farnsworth–Munsell 100-Hue and Dichotomous Tests for Color Vision." *Journal of the Optical Society of America* 33 (10): 568–574.
- Florêncio, D., and C. Herley. 2007. "A Large-Scale Study of web Password Habits." Proceedings of the 16th International Conference on World Wide Web. ACM, 657–666.
- Florêncio, D., and C. Herley. 2010. "Where Do Security Policies Come From?" In Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS' 10), ACM, New York, NY, 10. doi:10.1145/1837110.1837124.
- Forget, A., S. Chiasson, and R. Biddle. 2008. "Lessons from Brain Age on Password Memorability." Proceedings of the 2008 Conference on Future Play: Research, Play, Share, ACM, Toronto, Canada, 262–263.
- Furnell, S., K. Helkala, and N. Woods. 2022. "Accessible Authentication: Assessing the Applicability for Users with Disabilities." *Computers & Security* 113: 102561.
- Gao, X., Y. Yang, C. Liu, C. Mitropoulos, J. Lindqvist, and A. Oulasvirta. 2018. "Forgetting of Passwords: Ecological Theory and Data." Proceedings of 27th USENIX Security Symposium (USENIX Security 18), 221–238.
- Gaw, S., and E. Felten. 2006. "Password Management Strategies for Online Accounts." Proceedings of the Second Symposium on Usable Privacy and Security, (SOUPS), ACM, New York, NY, 44–55. doi:10.1145/1143120.1143127.
- Grawemeyer, B., and H. Johnson. 2011. "Using and Managing Multiple Passwords: A Week to a View." *Interacting with Computers* 23: 256–267. doi:10.1016/j.intcom.2011.03.007.
- Guo, K. H. 2013. "Security-related Behavior in Using Information Systems in the Workplace: A Review and Synthesis." *Computers & Security* 32: 242–251. <http://doi.org/10.1016/j.cose.2012.10.003>.
- Guo, K. H., and Y. Yuan. 2012. "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model." *Information & Management* 49 (6): 320–326.
- Habib, H., P. E. Naeni, S. Devlin, M. Oates, C. Swoopes, L. Bauer, and L. F. Cranor. 2018. "User Behaviors and Attitudes Under Password Expiration Policies." Proceedings of Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), 13–30.
- Hanna, A., and G. R. Loftus. 1993. "A Model for Conceptual Processing of Naturalistic Scenes." *Canadian Journal of Experimental Psychology* 47: 548–569.
- Hanna, A., and R. Remington. 1996. "The Representation of Color and Form in Long-Term Memory." *Memory & Cognition* 24 (3): 322–330.
- Haque, S. T., M. N. Al-Ameen, S. Scielzo, and M. Wright. 2017. "Learning System-assigned Passwords (up to 56 Bits) in a Single Registration Session with the Methods of Cognitive Psychology." Proceedings of the USEC '17, San Diego, CA: The Internet Society, 1–10, <http://doi.org/10.14722/usec.2017.23034>.
- Hartwig, K., and C. Reuter. 2021. "Nudging Users Towards Better Security Decisions in Password Creation Using Whitebox-based Multidimensional Visualisations." *Behaviour & Information Technology* 41 (7): 1357–1380.
- Hayashi, E., B. A. Pendleton, F. K. Ozenc, and J. I. Hong. 2012. "WebTicket: Account Management Using Printable Tokens." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2012, ACM, New York, NY, 997–1006.
- Helkala, K., and N. K. Svendsen. 2011. "The Security and Memorability of Passwords Generated by Using an Association Element and a Personal Factor." Proceedings of the Nordic Conference on Secure IT Systems, Springer, Berlin Heidelberg, 114–130.
- Herath, T., and H. R. Rao. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations." *European Journal of Information Systems* 18 (2): 106–125.
- Herley, C., and P. Van Oorschot. 2012. "A Research Agenda Acknowledging the Persistence of Passwords." *IEEE Security & Privacy* 10 (1): 28–36.
- Hoonakker, P., N. Bornoe, and P. Carayon. 2009. "Password Authentication from a Human Factors Perspective: Results of a Survey Among End-Users." Proceedings of the Human Factors and Ergonomics Society Annual Meeting, SAGE, Vol. 53, No. 6, 459–463.
- Huang, K., C. Lin, and S. Chiang. 2008. "Color Preferences and Familiarity in Performance on Brand Logo Recall." *Perceptual and Motor Skills* 107: 587–596.
- Inglesant, P., and M. A. Sasse. 2010. "The True Cost of Unusable Password Policies: Password Use in the Wild." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2010, ACM, New York, NY, 383–392. doi:10.1145/1753326.1753384.
- Ishihara, S. 1917. "Tests for Color-blindness" (Handaya, Tokyo, Hongo Harukicho, 1917).
- Itten, J. 1973. *The Art of Color: The Subjective Experience and Objective Rationale of Color*. New York: Van Nostrand Reinhold.
- Ives, B., K. Walsh, and H. Schneider. 2004. "The Domino Effect of Password Reuse." *Communications of the ACM* 47 (4): 75–78. doi:10.1145/975817.975820.
- Jenkins, J. L., M. Grimes, J. Proudfoot, and P. B. Lowry. 2014. "Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Detering Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Warnings." *Information Technology for Development* 20 (2): 196–213.
- Johnston, A. C., M. Warkentin, and M. Siponen. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric." *MIS Quarterly* 39 (1): 113–134.
- Kawasaki, M., and Y. Yamaguchi. 2012. "Individual Visual Working Memory Capacities and Related Brain Oscillatory Activities Are Modulated by Color Preferences." *Frontiers in Human Neuroscience* 6: 318.
- Keith, M., B. Shao, and P. Steinbart. 2009. "A Behavioral Analysis of Passphrase Design and Effectiveness." *Journal of the Association for Information Systems* 10 (2): 63–89.
- Khamis, M., T. Seitz, L. Mertl, A. Nguyen, M. Schneller, and Z. Li. 2019. "Passquerade: Improving Error Correction of Text Passwords on Mobile Devices by Using Graphic Filters for Password Masking." Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1–8.

- Kharrufa, A., T. Ploetz, and P. Olivier. 2017. "A Unified Model for User Identification on Multi-Touch Surfaces: A Survey and Meta-Analysis." *ACM Transactions on Computer-Human Interaction (TOCHI)* 24 (6): 1–39.
- Komanduri, S., R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, ... S. Egelman. 2011, May. "Of Passwords and People: Measuring the Effect of Password-Composition Policies." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2595–2604.
- Legner, C., T. Eymann, T. Hess, C. Matt, T. Böhm, P. Drews, A. Mädche, N. Urbach, and F. Ahlemann. 2017. "Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community." *Business & Information Systems Engineering* 59 (4): 301–308.
- Liu, F., and M. D. Myers. 2011. "An Analysis of the AIS Basket of Top Journals." *Journal of Systems and Information Technology* 13 (1): 5–24.
- Livingstone, M. S., and D. H. Hubel. 1987. "Psychophysical Evidence for Separate Channels for the Perception of Form, Color, Movement, and Depth." *Journal of Neuroscience* 7: 3416–3468.
- Loreto, V., A. Mukherjee, and F. Tria. 2012. "On the Origin of the Hierarchy of Color Names." *PNAS* 109 (18): 6819–6824.
- Maier, M. A., P. Barchfeld, A. J. Elliot, and R. Pekrun. 2009. "Context Specificity of Implicit Preferences: The Case of Human Preference for Red." *Emotion* 9 (5): 734.
- Mamonov, S., and R. Benbunan-Fich. 2018. "The Impact of Information Security Threat Awareness on Privacy-Protective Behaviors." *Computers in Human Behavior* 83: 32–44.
- Marquardson, J. 2012. "Password Policy Effects on Entropy and Recall: Research in Progress." In Proceedings of the 8th Americas Conference on Information Systems (AMCIS), AISel, Seattle, Washington.
- Masui, T. 2013. "Episopass: Password Management Based on Episodic Memories." Proceedings of the 21st Workshop on Interactive Systems and Software (WISS2013) (pp. 109–114).
- Mazurek, M. L., S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur. 2013. "Measuring Password Guessability for an Entire University." *Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security* 173–186.
- Merdenyan, B., and H. Petrie. 2022. "Two Studies of the Perceptions of Risk, Benefits and Likelihood of Undertaking Password Management Behaviours." *Behaviour & Information Technology*, 1–14. Ahead of print.
- Nelson, D., and K. L. Vu. 2010. "Effectiveness of Image-Based Mnemonic Techniques for Enhancing the Memorability and Security of User-Generated Passwords." *Computers in Human Behavior* 26 (4): 705–715.
- Notoatmodjo, G., and C. Thomborson. 2009. "Passwords and Perceptions." Proceedings of the 7th Australasian Information Security Conference, AISC, Wellington, New Zealand.
- Paivio, A. 1971. *Imagery and Verbal Processes*. London: Holt Rinehart and Winston.
- Palmer, S. E., and K. B. Schloss. 2010. "An Ecological Valence Theory of Human Color Preference." *In Proceedings of the National Academy of Sciences* 107 (19): 8877–8882.
- Pasquini, D., M. Cianfriglia, G. Ateniese, and M. Bernaschi. 2021. "Reducing Bias in Modeling Real-World Password Strength via Deep Learning and Dynamic Dictionaries." 30th USENIX Security Symposium (USENIX Security 21), 821–838.
- Peer, E., S. Egelman, M. Harbach, N. Malkin, A. Mathur, and A. Frik. 2020. "Nudge Me Right: Personalizing Online Security Nudges to People's Decision-Making Styles." *Computers in Human Behavior* 109: 106347.
- Poulin, R. 2011. *The Language of Graphic Design: An Illustrated Handbook for Understanding Fundamental Design Principles*. Beverly, MA: Rockport.
- Renaud, K., and A. De Angeli. 2009. "Visual Passwords: Cure-all or Snake-oil?" *Communications of the ACM* 52 (12): 135–140.
- Renaud, K., and J. Ramsay. 2014. "How Helpful is Colour-Cueing of PIN Entry?". Cornell University arXiv preprint arXiv:1407.8007.
- Ryan, G., and M. Valverde. 2006. "Waiting in Line for Online Services: A Qualitative Study of the User's Perspective." *Information Systems Journal* 16 (2): 181–211.
- Saastamoinen, A. 2014. "Lomalla unohtuneet salasana-työnantajille kalliiksi – jopa satojen tuhansien kustannukset." Accessed 24.09.15. http://yle.fi/ylex/uutiset/lomalla_unohtuneet_salasanat_tulevat_tyonantajille_kalliiksi_jopa_satojen_tuhansien_kustannukset/3-7580109.
- Sasse, M. A., S. Brostoff, and D. Weirich. 2001. "Transforming the 'Weakest Link' – a Human/Computer Interaction Approach to Usable and Effective Security." *BT Technological Journal* 19 (3): 122–131.
- Seitz, T., M. Hartmann, J. Pfab, and S. Souque. 2017. "Do Differences in Password Policies Prevent Password Reuse?" Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems, CHI EA '17, ACM, New York, NY, 2056–2063.
- Seo, B. G., and D. H. Park. 2019. "The Effect of Message Framing on Security Behavior in Online Services: Focusing on the Shift of Time Orientation via Psychological Ownership." *Computers in Human Behavior* 93: 357–369.
- Shay, R., L. Bauer, N. Christin, L. F. Cranor, A. Forget, S. Komanduri, Michelle L. Mazurek, William Melicher, Sean M. Segreti, and B. Ur. 2015, April. "A Spoonful of Sugar? The Impact of Guidance and Feedback on Password-Creation Behavior." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2903–2912.
- Shay, R., Saranga Komanduri, Adam L. Durity, Huh Phillip (Seyoung), Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. "Designing Password Policies for Strength and Usability." *ACM Transactions on Information and System Security (TISSEC)* 18 (4): 13–34.
- Shay, R., S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. 2010. "Encountering Stronger Password Requirements: User Attitudes and Behaviors." Proceedings of the 6th Symposium on Usable Privacy and Security, SOUPS' 10, ACM, New York, NY, 2.
- Siponen, M., and A. Vance. 2014. "Guidelines for Improving the Contextual Relevance of Field Surveys: The Case of Information Security Policy Violations." *European Journal of Information Systems* 23 (3): 289–305.

- Stobert, E., and R. Biddle. 2014. "A Password Manager That Doesn't Remember Passwords." Proceedings of the 2014 New Security Paradigms Workshop, NSPW '14, ACM, New York, NY, 39–52.
- Tam, L., M. Glassman, and M. Vandenwauver. 2010. "The Psychology of Password Management: A Tradeoff Between Security and Convenience." *Behaviour & Information Technology* 29 (3): 233–244.
- Taylor, C., A. Clifford, and A. Franklin. 2013. "Color Preferences Are Not Universal." *Journal of Experimental Psychology: General* 142 (4): 1015–1027.
- Thoopsamut, P., and B. Limthanmaphon. 2019. "Handwritten Signature Authentication Using Color Coherence Vector and Signing Behavior." Proceedings of the 2019 2nd International Conference on Information Science and Systems, 38–42.
- Tulving, E., and D. Thomson. 1973. "Encoding Specificity and Retrieval Processes in Episodic Memory." *Psychological Review* 80 (5): 352–373.
- Ur, B., J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor. 2016. "Do Users' Perceptions of Password Security Match Reality?" Proceedings of the CHI Conference on Human Factors in Computing Systems, CHI'16, ACM, New York, NY, 3748–3760. doi:10.1145/2858036.2858546.
- Vance, A., D. Eargle, K. Ouimet, and D. Straub. 2013. "Enhancing Password Security Through Interactive Fear Appeals: A Web-based Field Experiment." Proceedings of 46th Hawaii International Conference on System Sciences (HICSS), Hawaii: IEEE, 2988–2997. doi:10.1109/HICSS.2013.196.
- van Oorschot, P. C., and J. Thorpe. 2008. "On Predictive Models and User-Drawn Graphical Passwords." *ACM Transactions on Information and System Security (TISSEC)* 10 (4): 1–33.
- Vu, K. L., R. W. Proctor, A. Bhargav-Spantzel, B. Tai, J. Cook, and E. E. Schultz. 2007. "Improving Password Security and Memorability to Protect Personal and Organizational Information." *International Journal of Human-Computer Studies* 65: 744–757. <https://doi.org/10.1016/j.ijhcs.2007.03.007>.
- Wang, D., P. Wang, D. He, and Y. Tian. 2019. "Birthday, Name and Bifacial-Security: Understanding Passwords of Chinese web Users." 28th USENIX Security Symposium (USENIX Security 19), 1537–1555.
- Wang, D., Z. Zhang, P. Wang, J. Yan, and X. Huang. 2016. "Targeted Online Password Guessing: An Underestimated Threat." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 1242–1254.
- Weir, C. S., G. Douglas, M. Carruthers, and M. Jack. 2009. "User Perceptions of Security, Convenience and Usability for ebanking Authentication Tokens." *Computers & Security* 28 (1): 47–62.
- Wichmann, F. A., L. T. Sharpe, and K. R. Gegenfurtner. 2002. "The Contributions of Color to Recognition Memory for Natural Scenes." *Journal of Experimental Psychology: Learning, Memory, and Cognition* 28 (3): 509–520.
- Wiedenbeck, S., J. Waters, J. Birget, A. Brodskiy, and N. Memon. 2005. "PassPoints: Design and Longitudinal Evaluation of a Graphical Password System." *International Journal of Human-Computer Studies* 63: 102–127.
- Woo, S., R. Artstein, E. Kaiser, X. Le, and J. Mirkovic. 2019. "Using Episodic Memory for User Authentication." *ACM Transactions on Privacy and Security (TOPS)* 22 (2): 1–34.
- Woods, N. 2017. "Frequently Using Passwords Increases Their Memorability – A False Assumption or Reality?" Proceedings of the 23rd Americas Conference on Information Systems (AMCIS 2017), AISel, Boston, MA, 1–5.
- Woods, N. 2022. "Users' Psychopathologies: Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior." In *Cyber Security*, 93–134. Cham: Springer.
- Woods, N., and M. Siponen. 2018. "Too Many Passwords? How Understanding our Memory Can Increase Password Memorability." *International Journal of Human-Computer Studies* 111: 36–48.
- Woods, N., and M. Siponen. 2019. "Improving Password Memorability, While Not Inconveniencing the User." *International Journal of Human-Computer Studies* 128: 61–71.
- Workman, M., W. H. Bommer, and D. Straub. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test." *Computers in Human Behavior* 24: 2799–2816.
- World Internet Users Statistics. 2019. Accessed: 01/05/2019, <http://www.internetworldstats.com/stats.htm>.
- Wyler, S. 1992. *Colour and Language: Colour Terms in English*, Vol. 364. Tübingen: Gunter Narr Verlag.
- Yang, W., N. Li, O. Chowdhury, A. Xiong, and R. W. Proctor. 2016. "An Empirical Study of Mnemonic Sentence-Based Password Generation Strategies." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications security, CCS '16, ACM, New York, NY, 1216–1229.
- Zeki, S. 1993. *A Vision of the Brain*. Oxford: Blackwell.
- Zeki, S. M., and L. Marini. 1998. "Three Cortical Stages of Colour Processing in the Human Brain." *Brain* 121: 1669–1685.
- Zhang, J., X. Luo, S. Akkaladevi, and J. Ziegelmayr. 2009. "Improving Multiple Password Recall: An Empirical Study." *European Journal of Information Systems* 18 (2): 165–176.