Instructions for Creating Passwords: How do They Help in Password Creation

Saja Althubaiti
Human Computer Interaction Research Group
Department of Computer Science
University of York, York UK YO10 5GH
saaa505@york.ac.uk

Helen Petrie
Human Computer Interaction Research Group
Department of Computer Science
University of York, York UK YO10 5GH
helen.petrie@york.ac.uk

User instructions in the form of password policy or creation suggestion play an important role in helping users understand and comply with the requirements of a password creation system (PCS). Current implementations of user instructions are very varied and may cause users confusion as they move from one PCS to another which can in turn affect their password choice. Therefore, this paper investigates what kinds of instructions are provided by PCSs to support users in creating passwords and how the most frequently used instructions affect users' password creation behaviour. An analysis of a total of 95 instructions were extracted from 27 PCSs was undertaken. Based on this analysis, an online study with 117 respondents investigated how the most frequently used instructions affect users' password creation behaviour. The results revealed that current implementations of user instructions for password policy and creation suggestion in the PCSs do not match users' need in creating passwords. Users prefer declarative policy before they interact with a PCS. However, they prefer procedural policy during and after their interaction with a PCS. For creation suggestions, users prefer declarative suggestions before, during and after interaction with a PCS.

Password Creation Instructions. Password Policy. Password Creation Suggestions.

1 INTRODUCTION

Textual passwords are still widely used and continue to be a problem for users and a major concern for the online security community. In spite of advances in graphical passwords (Biddle et al., 2012) and biometric authentication (Jain and Kumar, 2012), most users seem burdened with many textual passwords which they need to use and remember across many different systems. A diary study by Grawemeyer and Johnson (2011) found that in a one-week period, a sample of 22 well-educated participants used passwords over 45 times each, with approximately eight different passwords.

Many studies have shown that the weaknesses in passwords result primarily from users' behaviour (e.g. Brown et al. 2004; Sasse et al. 2001). They often sacrifice security for convenience (Tam et al. 2010). For instance, to remember passwords users tend to choose easy-to-remember but easy-to-crack passwords. Thus, choosing a good password, which is both strong and memorable, is the first stage of changing users' behaviour.

Users create passwords with what can be considered small interactive systems consisting of one or more screens, which include user instructions about password policy (a set of rules that determine the accepted content of passwords) and password creation suggestions (which advise users on the content of good passwords). Such Password Creation Systems (PCSs) are considered as a particular class of interactive system that offer supporting features to help users achieve a certain level of security during the password creation process.

The need to support users to choose usable and secure textual passwords has been clearly noted in the literature. Previous studies have focused on examining the security and memorability of chosen passwords rather than looking at what kinds of instructions users find helpful when creating passwords and their effect on users' performance.

To our knowledge, none of the previous studies has looked at the user instructions provided in the PCSs from the user perspective. Yet user instructions in the form of password policy or creation suggestion play a key role in helping users understand and comply with a PCS's requirements. In fact, current implementations of user instructions are very varied and this may cause users confusion as they move from one PCS to another which can in turn affect their password choice. Furthermore, current guidance provided by PCSs often does not seem effective for users when choosing a password. Results from Florencio and Herley (2007) indicated that users continue to tend to choose weak

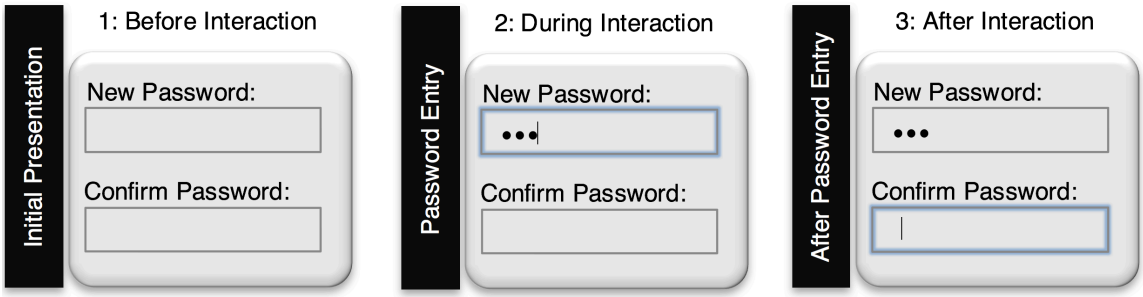

Figure 1: *The three-step model of PCS*

passwords. Therefore, studying user instructions in PCSs and ensuring they support users well when creating passwords is very important.

This paper, therefore, aims to provide a better understanding of the user instructions provided in PCSs by firstly analysing existing user instructions to support users in creating passwords from a sample of 27 current PCSs. To understand how the most frequently used instructions actually affect users' password creation behaviour, an online study was then conducted. During the study, 117 respondents rated and commented on different possible instructions in the context of creating a password.

2 BACKGROUND AND RELATED WORK ON USER INSTRUCTIONS

Generally, user instructions are classified into declarative information and procedural information (Ummelen, 1997). Declarative information provides exploratory information whereas procedural information is concerned with actions. However, the use and effects of the two types in user instructions are not very clear (Karreman et al., 2005).

Carroll and Mack (1984) concluded that user instructions have to be action-centred. Since users tend to learn by doing and not by reading instructions. However, positive effects of declarative information have been found when users were forced to read this type of information (Smith and Goodman, 1984). Furthermore, results from Karreman et al. (2005) indicated that reading declarative information leads to positive effects on task performance but negatively affected users' confidence.

One way to solve this problem would be to provide both declarative and procedural information in user instructions. However, redundant information resulted in higher cognitive load (Sweller and Chandler 1991). For thus, providing the right type of information at the right time for users to perform their task successfully is important.

3 PASSWORD CREATION SYSTEMS

PCSs are interactive web-based systems that incorporated in password protected websites. Most users interact with PCSs when they sign up for a website during the registration phase and if they forget their password. PCSs can provide a number of supporting features to help users choose passwords such as a strength meter, statement of password policy, suggestions for creating good passwords and feedback to users about weak passwords or violations of policy in their proposed passwords.

An analysis of existing PCSs leads us to conceptualize the password creation process in a three-step model. The three interaction steps in most PCSs are as follows: (1) *before-interaction* which is the initial presentation before the users start creating a password, so when they open the page with the field for entering the password; a this step a password policy or suggestions for good passwords may be presented (2) *during-interaction* which is the password entry step; at this step dynamic information may be presented about the strength or appropriateness of the password as it is entered (3) *after-interaction* when feedback may be given about the new password after has been entered in full. Figure 1 illustrates the three steps in the model.

4 STUDY 1: ANALYSIS OF CURRENT INSTRUCTIONS FOR CREATING PASSWORDS

An analysis was undertaken of a sample of current PCSs in order to understand what kinds of instructions are provided by PCSs to support users in creating passwords.

4.1 Data sources and coding scheme

A set of 27 websites with PCSs was selected from the top 100 entries on Alexa (Alexa Internet). Criteria for inclusion were: website should be in English; website should have a dedicated PCS (i.e. not use

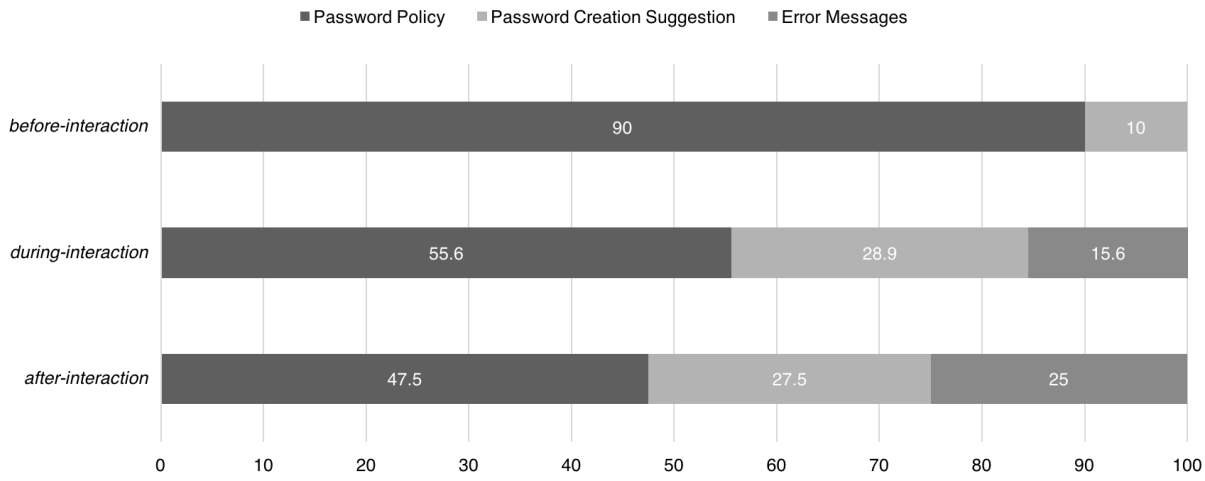

Figure 2: *The percentage of the temporal organization of the three types of instructions*

other systems such Google or Facebook); and PCS should not generate passwords automatically for users. These PCSs provided a range of different kinds of instructions at the three steps of interaction that guide users when they create new passwords. A total of 95 instructions were extracted and a content analysis was conducted on them.

An open coding technique was used. Seven attributes emerged from the coding. The seven attributes are:

Instruction type: password policy, password creation suggestion, and error message.

Explicit vs. Implicit: whether the instruction is given as an explicit statement or command to the user ("*Password needs at least one lowercase letter*", GitHub) or implicitly ("*at least 6 characters*", Amazon).

Procedural vs. Declarative: the grammatical form of the instruction. Four grammatical forms were found: declarative, phrasal, modal, and impetrative. The first three forms relate to users' declarative knowledge whereas the last one relates to procedural knowledge. Examples of the four forms are: declarative statement ("*Good passwords are hard to guess*", Dropbox); phrasal statement ("*8 character minimum, case sensitive*", Live); modal statement ("*Must contain at least 1 more characters"*, Stackoverflow); imperative statement ("*Include at least 1 number or symbol (like !@#$%^)*", PayPal).

Password-oriented vs. Action-oriented: this attribute identifies whether the instruction is stated in language related to the password or to an action users should (not) take in making their password. A password-oriented instruction is "*Short passwords are easy to guess*" (Google), whereas an action-oriented instruction is "*Avoid using the same password for multiple sites*" (eBay).

General vs. Specific: this attribute identifies the level of detail in the instruction. An example of general instruction is "*Please create a password for your account*" (DisneyStore). On the other hand, "*Your password is too short*" (Pinterest) is an example of specific instruction.

Positive vs. Negative: this attribute identifies whether the instruction used positive or negative instructions. Examples of negative instructions are: "*No consecutive identical characters*" (Outbrain), "*Don't use a password from another site or something too obvious like your pet's name*" (Google), and "*Your password is insecure*" (BBC).

Polite-command vs. Direct-command: this attribute looks at the politeness element of the instruction. The instruction was considered polite when it had the word 'please' in the statement (no other politeness forms were found in the instructions).

Both authors coded all the instructions, separately and together until there was complete agreement on the coding.

4.2 Results: current state of instructions for creating passwords

Only 10% of instructions were provided at the *before-interaction* step (10, 10.5%). Nearly half of the instructions were presented at the *during-interaction* step of the PCS (45, 47.4%), and about 40% at the *after-interaction* step (40, 42.1%). The temporal organization of the types of instruction is presented in Figure 2.

4.2.1 Instructions at the before-interaction step

The instruction types presented at the *before-interaction* were password policy and password creation suggestions, not strength meters. However, 90% (9/10) were password policies and only one was a password creation suggestion (1/10). Thus at

this stage PCSs support users only with information about what is needed rather than what makes a good password.

Looking more closely to the policy statements (n = 9), most of them were written implicitly (7/9). In addition, the use of declarative format (6/9) was more common than procedural format (3/9). With respect to the declarative format, there were phrasal (5/6) and declarative (1/6) sentences. Regarding password creation suggestions, the one instance of this instruction type which was written explicitly using a declarative sentence.

In general, it was found that almost all instructions presented *before-interaction* were specific and positive in format. Also, there was no occurrence of the politeness element with the procedural knowledge.

4.2.2 Instructions at the during-interaction step
The instruction types presented *during-interaction* included password policy, password creation suggestions and error messages. Again, the policy had the highest percentage with 55.6% (25/45), followed by password creation suggestions with 28.9% (13/45) and error messages with 15.6% (7/45).

For policy statements (n = 25), more than half of them was written explicitly (56.0%, 14/25). The use of declarative format (84.0%, 21/25) was much more common than procedural format (16.0%, 4/25). The declarative format used modal (38.1%, 8/21), phrasal (33.3%, 7/21), and declarative (28.6%, 6/21) sentences. In addition, the policy statements used both positive and negative in both declarative and procedural formats (except for the modal sentences which was only stated in positive tone). All instruction types that related to policy were specific. The majority of password creation suggestions (n = 13) were written explicitly (76.9%, 10/13). Procedural format (61.5%, 8/13) was more common than declarative format (38.6%, 5/13). The declarative format instructions using only declarative sentences. When the suggestions were declarative they more general (60.0%, 3/5) than specific (40.0%, 2.5), but numbers here are very small. In contrast, when they were procedural they tended to be more specific (62.5%, 5/8) than general (37.5%, 3/8), again the numbers are small.

Negative constructions appeared only with the procedural format. Also, the politeness element appeared only with the positive procedural format.

4.2.3 Instructions at the after-interaction step
The instruction types presented *after-interaction* were similar to instructions presented in the *during-interaction step.* Password policy had the highest percentage with 47.5% (19/40), followed by the creation suggestions with 27.5% (11/40) and error messages with 25% (10/40).

For policy statements (n = 19), more than half of them were written explicitly (73.7%, 14/19). The use of declarative format (68.4%,13/19) was dominant than procedural knowledge (6/19). For the declarative format instructions, modal sentences (92.3%, 12/13) were much more common than declarative sentences (76.9%, 1/13). In addition, the policy statements were written only using positive wording. All instruction types that related to policy were specific. The politeness element was used quite frequently in the procedural format (66.7%, 4/6), although numbers are small. Turning now to the password creation suggestions (n = 11), all of them were written explicitly in procedural format. General suggestions statements (81.8%, 9/11) were much more common than specific ones (18.2%, 2/11). All statements of suggestions were presented as positive. Also, nearly three-quarters of the them were written with the use of politeness element (72.7%, 8/11).

To understand how the most frequently used instructions actually affect users' password creation behaviour, an online questionnaire study was conducted, based on these analyses. However, the results of password policy and password creation suggestion will be reported as types of instructions in this paper.

5 STUDY 2: USER STUDY ON INSTRUCTIONS FOR CREATION PASSWORDS

This study investigated what forms of instructions users prefer for the statement of password policy and password creation suggestions across the three different steps of interaction with a PCS (*see* Section 3). A user study was conducted using an online questionnaire in which respondents were asked to rate and comment on a number of different possible instructions in the context of creating a password.

5.1 Method

5.1.1 Design
The study had three independent variables. The first independent variable is the of type of instructions with two conditions: *policy* and *creation suggestion*. The second independent variable is the type of format of the instructions with two conditions: *declarative* and *procedural*. The third independent variable is the timing of presentation with three conditions: at the *before-interaction step*, the *during-interaction* step, and the *after-interaction* step.

A total of 50 instructions statements were investigated. Due to the large number of statements, it was decided to divide the statements into three between respondent groups. Each group answered a questionnaire that had between 14 to 18 different instruction statements which took approximately 20 minutes to complete. The division of the group was

not meant to create a between-group comparison but to accommodate the large number of instruction to be investigated.

Table 1 illustrates the number of statements for each instruction type with the timing of presentation for each group. Each respondent in Group 1 received 14 statements of password policy under *before-interaction* and *during-interaction* conditions. Each respondent in Group 2 received 18 statements of password creation suggestions under *before-interaction* and *during-interaction* conditions. Each respondent in Group 3, received a total of 10 statements about password policy and creation suggestions under *after-interaction* condition.

Table 1: *The number of statements for each type of instruction with the timing of presentation in each group*

		Group 1	Group 2	Group 3*
before-interaction	*Policy*	**5**	**-**	**-**
	Declarative	2		
	Procedural	3		
	Creation Suggestion	**-**	**9**	**-**
	Declarative		4	
	Procedural		5	
during-interaction	*Policy*	**9**	**-**	**-**
	Declarative	6		
	Procedural	3		
	Creation Suggestion	**-**	**9**	**-**
	Declarative		3	
	Procedural		6	
after-interaction	*Policy*	**-**	**-**	**6**
	Declarative			3
	Procedural			3
	Creation Suggestion	**-**	**-**	**4**
	Declarative			1
	Procedural			3
Total		**14**	**18**	**10**

* In Group 3, there was 18 statements but only statements about password policy and creation suggestion are reported in this paper.

The instructions were presented in the context of an imaginary online service provided PCS. Respondents were asked to imagine their need to create a new password using this PCS.

There were four dependent variables: participants' ratings on 5-likert scale of (1) perceived helpfulness of instruction, (2) perceived clarity of instruction, (3) perceived amount of detail of instruction, and (4) participant's confidence about creating a password after reading the instruction.

5.1.2 Respondents

A total of 117 respondents took part in the study. The respondents were recruited from the University of York, Social Networks and Amazon Mechanical Turk (MTurk) crowdsourcing platform. The recruitment methods were varied to increase the range of respondents, the number of participation per group and to balance the sample size across the three groups.

In Group 1, there were 40 respondents all of whom were recruited from the Department of Computer Science at the University of York. In Group 2, there were 15 respondents (Non-MTurkers) from the Department of Theatre, Film and Television and the Department of Management and Law at the University of York and 19 respondents (MTurkers) from MTurk. In Group 3, there were 18 respondents (Non-MTurkers) from Social Networks and 25 respondents (MTurkers) from MTurk.

For Group 2 and Group 3, we tested the difference between Non-MTurkers and MTurkers; we found no significant difference in the results between the two groups of respondents. For thus, the data from Non-MTurkers and MTurkers in each group was combined for further analysis.

Overall, there were 49 (41.9%) females and 68 (58.1%) males. The respondents ranged in age from 19 to 68 years, with a mean age of 36.3 years (*SD* = 12.4). A majority of respondents (92, 78.6%) were native speakers of English whereas the remaining have been speaking English for 17.8 years (*SD* = 15). Almost half of the respondents (58, 49.7%) have a postgraduate degree. The level of education of the remaining respondents ranged from bachelor degree (42, 35.9%) to school degree (7, 6%). In general, the respondents' major/career background were divided evenly between computing (56, 47.9%) and non-computing (61, 52.1%) fields. On average, the majority of respondents spent more than 6 hours a day online and using computers.

Table 2 summarises the demographic characteristics of the respondents per group. As shown in the table, the overall respondent's characteristic does not differ between the three groups; except for the education level and major/career background. Most of the respondents in Group 2 and Group 3 have a bachelor degree. For the major/career background, most of respondents in Group 2 were from non-computing fields.

Table 2: *Demographic characteristics of respondents*

Characteristics	Frequency (%)		
	Group 1 (n = 40)	Group 2 (n = 34)	Group 3 (n = 43)
Gender			
Female	16 (40.0)	13 (38.2)	20 (46.5)
Male	24 (60.0)	21 (61.8)	23 (53.5)
Language			
English	25 (62.5)	30 (88.2)	37 (86.0)
Other	15 (37.5)	4 (11.8)	6 (14.0)
Education			
School	1 (2.5)	5 (14.7)	1 (2.3)
Diploma	1 (2.5)	2 (5.9)	7 (16.3)
Bachelor's	4 (10.0)	21 (61.8)	17 (39.5)
Master's	16 (40.0)	5 (14.7)	13 (30.2)
Doctoral	18 (45.0)	1 (2.9)	5 (11.6)
Major/Career			
Computing	30 (75.0)	6 (17.6)	20 (46.5)
Non-computing	10 (25.0)	28 (82.4)	23 (53.5)

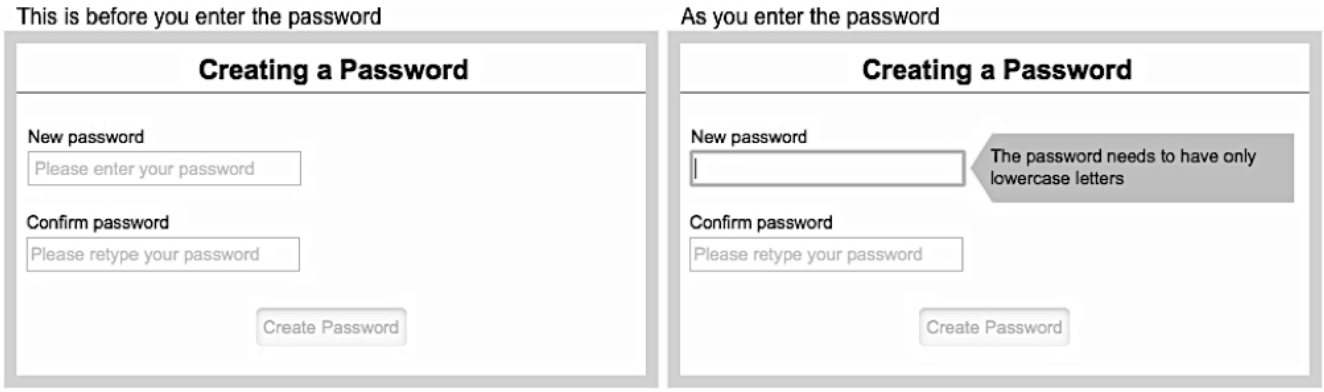

Figure 3: *An image of PCS that presents a password policy statement under during-interaction condition*

The participation was voluntary for some respondents and compensated by others. Specifically, respondents in Group 1 voluntarily participated in the study. For Group 2 and Group 3, respondents were compensated in the form of USD 0.50 (equivalent to GBP 0.40) for MTurkers and as prize draw of 10 Amazon vouchers worth GBP 10 for non-MTurkers.

5.1.3 Materials

The materials will be described for each group. However, there are common characteristics between the questionnaires for each group. All questionnaires had the same structure; they began with a briefing that covered the overall purpose of the study and they ended with demographic questions. The timing of presentation factor was used to split the set of statements within each group. Before presenting each timing of presentation condition, an introduction page was provided. The introduction page described the condition which respondents were about to experience and the user instructions for creating the password using the PCS.

In addition, an image of PCS with the password policy or creation suggestion was provided for each statement respondents received in order to help them visualise the PCS. Figure 3 shows an example of the image presented for a password policy statement under *during-interaction* condition.

For Group 1, the questionnaire consisted of 14 statements of password policy in the *before-interaction* and *during-interaction* conditions. All policy statements in the *before-interaction* condition used the following policy: “have at least six characters and at least one numeral“. There were 5 variations created to present this policy (2 declarative and 3 procedural). For the *during-interaction* condition, the policy statements addressed the following policy: “has lowercase letters only”. There were 9 variations of stating this policy (6 declarative and 3 procedural). Examples of the policy statements used in *before-interaction* and *during-interaction* conditions are:

1. The password needs to have at least six characters and at least one numeral. (*policy*, *declarative*, *before-interaction*);
2. Use at least six characters and at least one numeral. (*policy*, *procedural*, *before-interaction*);
3. The password must have only lowercase letters. (*policy*, *declarative*, *during-interaction*);
4. Use only lowercase letters. (*policy*, *procedural*, *during-interaction*).

For Group 2, the questionnaire consisted of 18 statements of password creation suggestions in the *before-interaction* and *during-interaction* conditions. For the *before-interaction* condition, all suggestion statements provided the following suggestion: “you use both letters and numbers or only uncommon words”. There were 9 variations of this suggestion (4 declarative and 5 procedural). For the *during-interaction* condition, the suggestion statements provided this following advice: “your password will be better if you add symbols or jokes” with 9 variations were created (3 declarative and 6 procedural). Examples of the creation suggestion statements used in *before-interaction* and *during-interaction* conditions are:

1. Good passwords have uncommon words. (*suggestion*, *declarative*, *before-interaction*);
2. Use both letters and numbers to make a good password. (*suggestion*, *procedural*, *before-interaction*);
3. You can improve your password by adding jokes. (*suggestion*, *declarative*, *during-interaction*);
4. Add symbols to make your password stronger. (*suggestion*, *procedural*, *during-interaction*).

For Group 3, the questionnaire consisted of 10 statements of password policy and creation suggestions, all in the *after-interaction* condition. There were 6 policy statements and 4 suggestion statements. For the policy statements, the following policy was used: “your password should have a

Table 3: *Mean (median) ratings of the perceived helpfulness, clarity, amount of details and respondents' confidence of the declarative and procedural policy and creation suggestions presented at the before-interaction step; (1-5, Higher = Better)*

		Helpfulness	Clarity	Amount of details	Confidence
		Password Policy			
	Declarative	3.78 (4.00)	3.75 (4.00)	2.70 (2.75)	3.93 (4.00)
	Procedural	3.58 (3.67)	3.43 (3.50)	2.69 (2.83)	3.76 (3.67)
before-interaction step	**p value**	**.010**	**.006**	**n.s.**	**.031**
		Password Creation Suggestion			
	Declarative	2.78 (2.75)	3.15 (3.25)	2.41 (2.50)	2.99 (3.00)
	Procedural	2.39 (2.40)	2.75 (2.70)	2.08 (2.20)	2.54 (2.40)
	p value	**.000**	**.001**	**.000**	**.000**

combination of uppercase, lowercase, and symbols."; 3 declarative and 3 procedural statements were created. The suggestion statements addressed the following advice: "your password has at least eight characters" with 1 declarative and 3 procedural statements. Examples of the statements of the two types of instructions used in *after-interaction* condition:

1. The password should be a combination of uppercase letters, lowercase letters, and symbols. (*policy, declarative, after-interaction*);
2. Do not use only uppercase letters, lowercase letters, and symbols. (*policy, procedural*, *after-interaction*);
3. Good passwords have at least eight characters. (*suggestion, declarative*, *after-interaction*);
4. Please try one with at least eight characters. (*suggestion, procedural*, *after-interaction*).

5.1.4 Procedure

Links to the three questionnaires were distributed via e-mailing lists, social networks and the MTurk platform. A briefing about the study and an informed consent form was given at the beginning of the questionnaire. Respondents were assured that they would not be asked to reveal any of their passwords or create any passwords. Respondents then confirmed their agreement and their understanding of the information provided in the briefing by clicking on the 'Next' button. After that, respondents were asked to imagine their need to create a new password using a PCS. The instructions were presented in the context of an imaginary online service provided PCS. They were instructed to read the user instruction provided in the PCS and then answer a simple set of questions about the user instructions. Upon completing of the questionnaire, respondents were asked to answer demographic questions.

5.2 Results

For this paper, a set of within-participant analyses was performed for each group to compare participants' performance on between the two types of format conditions: *declarative* and *procedural*. Wilcoxon Signed-ranks test were used for the within-participant analyses.

5.2.1 Ratings of instructions at the before-interaction step

Table 3 shows the mean (and median) ratings for the perceived helpfulness, clarity, amount of details and respondents' confidence of the *policy* and *suggestion* provided at the *before-interaction* step.

For the ratings of helpfulness, there was a significant difference in ratings between the two types of format of the instructions for the *policy* instructions ($Z = -2.56$, $p = .010$) and *suggestion* instructions ($Z = -3.63$, $p < .001$). Respondents rated the helpfulness of the *declarative* format significantly higher than the *procedural* format for both *policy* and *suggestion* instructions.

For the ratings of clarity, there was a significant difference in ratings between the two types of format of the instructions for the *policy* instructions ($Z = -2.74$, $p = .006$) and *suggestion* instructions ($Z = -3.30$, $p = .001$). Respondents rated the clarity of the *declarative* format significantly higher than the *procedural* format for both *policy* and *suggestion* instructions.

For the ratings of the amount of details, there was a significant difference in ratings between the two types of format of the instructions in the *suggestion* instructions ($Z = -4.12$, $p < .001$), but not the *policy* instructions ($Z = .22$, n.s.). The ratings of amount of details in *declarative* suggestion presented was significantly higher than *procedural* suggestion.

For the ratings of confidence, there was a significant difference in ratings between the two types of format of the instructions for the *policy* instructions ($Z = -2.16$, $p = .031$) and *suggestion* instructions ($Z = -4.07$, $p < .001$). In both types of instructions, respondents felt more confident reading the *declarative* format than *procedural* format.

Table 4: *Mean (median) ratings of the perceived helpfulness, clarity, amount of details and respondents' confidence of the declarative and procedural policy and creation suggestions presented at the during-interaction step; (1-5, Higher = Better)*

		Helpfulness	**Clarity**	**Amount of details**	**Confidence**
		Password Policy			
during-interaction step	Declarative	2.93 (3.00)	3.07 (3.17)	2.40 (2.50)	3.22 (3.17)
	Procedural	3.38 (3.33)	3.63 (3.67)	2.63 (2.67)	3.54 (3.67)
	p value	**.000**	**.000**	**.000**	**.000**
	Password Creation Suggestion				
	Declarative	2.82 (2.67)	2.96 (3.00)	2.26 (2.33)	2.86 (2.67)
	Procedural	2.35 (2.25)	2.48 (2.58)	1.98 (2.00)	2.33 (2.17)
	p value	**.000**	**.000**	**.003**	**.000**

5.2.2 Ratings of instructions at the during-interaction step

Table 4 shows the mean (and median) ratings for the perceived helpfulness, clarity, amount of details and respondents' confidence of the *policy* and *suggestion* provided at the *during-interaction* step.

For the ratings of helpfulness, there was a significant difference in ratings between the two types of format of the instructions for the *policy* instructions ($Z = -4.41$, $p < .001$) and *suggestion* instructions ($Z = -4.23$, $p < .001$). Respondents rated the helpfulness of the *procedural* policy significantly higher than *declarative* policy, whereas, they rated the helpfulness of the *declarative* suggestion significantly higher than *procedural* suggestion.

For the ratings of clarity, there was a significant difference in ratings between the two types of format of the instructions for both the *policy* instructions ($Z = -4.57$, $p < .001$) and *suggestion* instructions ($Z = -4.06$, $p < .001$). The *procedural* policy was significantly clearer than *declarative* policy. On the other hand, the *declarative* suggestion was significantly clearer than *procedural* suggestion.

For the ratings of the amount of details, there was a significant difference in ratings between the two types of format of the instructions for both the *policy* instructions ($Z= -3.93$, $p < .001$) and *suggestion* instructions ($Z = -2.96$, $p = .003$). In the *policy* instructions, the ratings of amount of details in *procedural* format presented was higher than *declarative* format. Whereas, in the *suggestion* instructions, the ratings of amount of details in *declarative* format presented was higher than *procedural* format.

For the ratings of confidence, there was a significant difference in ratings between the two types of format of the instructions for the *policy* instructions ($Z = -4.12$, $p < .001$) and *suggestion* instructions ($Z = -4.35$, $p < .001$). Respondents were more confident reading *procedural* policy than *declarative* policy, on the other hand, they were more confident reading *declarative* suggestion than *procedural* suggestion.

5.2.3 Ratings of instructions at the after-interaction step

Table 5 shows the mean (and median) ratings for the perceived helpfulness, clarity, amount of details and respondents' confidence of the *policy* and *suggestion* provided at the after-interaction step.

For the ratings of helpfulness, there was a significant difference in ratings between the two types of format of the instructions for the *suggestion* instructions ($Z= -3.58$, $p < .001$), but not the *policy* instructions ($Z = -.248$, n.s.). In the *suggestion* instruction, respondents rated the helpfulness of *declarative* format significantly higher than *procedural* format.

For the ratings of clarity, there was a significant difference in ratings between the two types of format of the instructions for the *suggestion* instructions ($Z = -3.41$, $p = .001$), but not the *policy* instructions ($Z = -.802$, n.s.). In the *suggestion* instruction, respondents perceived *declarative* format to be more clearer than *procedural* format.

For the ratings of the amount of details, there was a significant difference in ratings between the two types of format of the instructions for the *suggestion* instructions ($Z = -2.81$, $p = .005$), but not the *policy* instructions ($Z = -1.44$, n.s.). In the *suggestion* instruction, the ratings of amount of details in *declarative* format presented was higher than *procedural* format.

For the ratings of confidence, there was a significant difference in ratings between the two types of format of the instructions for the *suggestion* instructions ($Z = -3.97$, $p < .001$), but not the *policy* instructions ($Z = -.526$, n.s.). In the *suggestion* instruction, respondents felt more confident reading the *declarative* format than *procedural* format.

6 DISCUSSION

The main aims of this paper were to understand what kinds of instructions are provided by PCSs to support users in creating passwords and to investigate how the most frequently used instructions actually affect users' password creation

Table 5: *Mean (median) ratings of the perceived helpfulness, clarity, amount of details and respondents' confident of the declarative and procedural policy and creation suggestions presented at the after-interaction step; (1-5, Higher = Better)*

		Helpfulness	**Clarity**	**Amount of details**	**Confidence**
after-interaction step	*Password Policy*				
	Declarative	3.41 (3.67)	3.46 (3.67)	2.49 (2.67)	3.44 (3.67)
	Procedural	3.45 (3.67)	3.53 (3.67)	2.56 (2.67)	3.39 (3.67)
	p value	**n.s.**	**n.s.**	**n.s.**	**n.s.**
	Password Creation Suggestion				
	Declarative	3.16 (3.00)	3.33 (3.00)	2.33 (2.00)	3.37 (3.00)
	Procedural	2.49 (2.33)	2.61 (2.33)	1.94 (1.67)	2.59 (2.33)
	p value	**.000**	**.001**	**.005**	**.000**

behaviour. To address these aims, an analysis of a total of 95 instructions extracted from 27 PCSs was carried out. Based on these analyses, an online questionnaire study with 117 respondents was conducted to understand how the most frequently used instructions actually affect users' password creation behaviour. It is interesting to compare the current practices of the implementation of user instructions from the analyses conducted (Study 1) with what was found from the online user study (Study 2).

The results revealed that only 10% of instructions were provided at the *before-interaction* step. It is somewhat surprising that so frequently there were no (or not enough) instructions for the user before they start creating a password. It seems possible to understand why users tend to make bad choices of passwords. Current PCSs do not provide enough support up front in terms of user instructions on how to create passwords which could have an influence on users' performance.

For the password policy, most user instructions provided at *before-interaction* step were declarative statements. The findings from the user study match the current practice of using declarative format for password policy. There was a significant difference in the levels of helpfulness, clarity, and users' confidence between the declarative and procedural policy. Respondents preferred declarative statements of password policy before their interaction with the PCSs.

Regarding password creation suggestion, there was few occurrences of this type of user instructions at *before-interaction* step in current PCSs. Thus, we examined both declarative and procedural suggestions. The results indicated a significant difference in the levels of helpfulness, clarity, amount of details and users' confidence between the declarative and procedural suggestion. Again, respondents preferred declarative statements of password creation suggestion before their interaction with the PCSs.

Nearly half of the analysed instructions were presented at the *during-interaction* step of the PCS. Most user instructions were password policy followed by password creation suggestion.

For the password policy, most user instructions presented at the *during-interaction* step were provided using declarative statements. However, the findings of the user study do not support the current practice of using declarative policy at this stage. Respondents preferred procedural statements of password policy during their interaction with the PCSs. There was a significant difference in the levels of helpfulness, clarity, amount of details and users' confidence between the declarative and procedural policy.

Turing to the password creation suggestion, most user instructions were written using a procedural format at the *during-interaction* step. However, the results from the user study do not support the current practice of using procedural format for creation suggestion at this stage. There was a significant difference in the levels of helpfulness, clarity, amount of details and users' confidence between the declarative and procedural suggestion. Respondents preferred declarative statements of password creation suggestion during their interaction with the PCSs.

The instruction types presented at the *after-interaction* step were similar to instructions presented at the *during-interaction* step. Most user instructions were password policy followed by the creation suggestions.

Regarding the password policy, similar to the previous two steps, most user instructions were declarative statements. Contrary to expectations, results from the user study showed no significant difference between the declarative and procedural policy at the *after-interaction* step. However, on average the ratings of procedural statements was higher than declarative statements in terms of the helpfulness, clarity and amount of details (except for the users' confidence).

For the password creation suggestion, most analysed user instructions at the *after-interaction* step were procedural format statements. The results from the user study differ from the current practice

of using procedural format. There was a significant difference in the levels of helpfulness, clarity, amount of details and users' confidence between the declarative and procedural suggestion. Respondents preferred declarative statements of password creation suggestion after their interaction with the PCSs.

In summary, the current implementation of user instructions for password policy and creation suggestion in the PCSs does not match the users' preferences for support instructions in creating passwords. Our results suggest the use of a declarative policy at *before-interaction* stage and the use of a procedural policy at *during-interaction* and at *after-interaction* stages. They also suggest the use of declarative suggestions through the password creation process regardless of the stage of interaction.

7 CONCLUSIONS AND FURTHER WORK

User instructions in the form of password policy or creation suggestion play a key role in helping users understand and comply with a PCS's requirements. If users are struggling to understand the instructions for creating good and secure passwords, this might affect the quality of the passwords they create. This paper shows that current implementations of user instructions are very varied and do not match users' needs. The results help us understand why users have difficulty choosing secure passwords.

However, these findings must be interpreted with caution because they are based on self-report data in an artificial password creation situation. Thus, further research is needed to better understand the effects of the user instructions on the user experience and the quality of the passwords.

8 ACKNOWLEDGEMENTS

The authors would like to thank all participants for their time. The first author thanks the Ministry of Education of Saudi Arabia for her PhD funding.

9 REFERENCES

Alexa Internet, The top 500 sites on the web. *Alexa*. Available at: http://www.alexa.com/topsites [Accessed February 1, 2016].

Biddle, R., Chiasson, S. and Van Oorschot, P.C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44, p.19.

Brown, A.S. et al. (2004). Generating and remembering passwords. *Applied Cognitive Psychology*, 18(6), pp.641–651.

Carroll, J. and Mack, R. (1984). Learning to use a word processor: By doing, by thinking, and by knowing. *Human factors in computer systems*.

Florencio, D. and Herley, C. (2007). A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web - WWW '07. New York, New York, USA: ACM Press, p. 657.

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

Jain, A.K. and Kumar, A. (2012). Biometric recognition: an overview. In E. Mordini and D. Tzovaras, eds. *Second Generation Biometrics: The Ethical, Legal and Social Context*. Springer, pp. 49–79.

Karreman, J., Ummelen, N. and Steehouder, M. (2005). Procedural and declarative information in user instructions: What we do and don't know about these information types. *… Conference*.

Sasse, M.A., Brostoff, S. and Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19, pp.122–131.

Smith, E.E. and Goodman, L. (1984). Understanding Written Instructions: The Role of an Explanatory Schema. *Cognition and Instruction*, 1(4), pp.359–396.

Sweller, J. and Chandler, P. (1991). Evidence for cognitive load theory. *Cognition and Instruction*, 8(4), pp.351–362.

Tam, L., Glassman, M. and Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour and Information Technology*, 29(3), pp.233–244.

Ummelen, N. (1997). *Procedural and declarative information in software manuals: Effects on information use, task performance and knowledge*, Rodopi.