Information & Computer Security

Must I, can I? I don't understand your ambiguous password rules

Kristen K. Greene Yee-Yin Choong

Must I, can I? I don't understand your ambiguous password rules

Kristen K. Greene and Yee-Yin Choong
National Institute of Standards and Technology, Gaithersburg, Maryland, USA

Received 24 June 2016
Revised 31 August 2016
Accepted 10 September 2016

Abstract

Purpose – The purpose of this research is to investigate user comprehension of ambiguous terminology in password rules. Although stringent password policies are in place to protect information system security, such complexity does not have to mean ambiguity for users. While many aspects of passwords have been studied, no research to date has systematically examined how ambiguous terminology affects user comprehension of password rules.

Design/methodology/approach – This research used a combination of quantitative and qualitative methods in a usable security study with 60 participants. Study tasks contained password rules based on real-world password requirements. Tasks consisted of character-selection tasks that varied the terms for non-alphanumeric characters to explore users' interpretations of password rule language, and compliance-checking tasks to investigate how well users can apply their understanding of the allowed character space.

Findings – Results show that manipulating password rule terminology causes users' interpretation of the allowed character space to shrink or expand. Users are confused by the terms "non-alphanumeric", "symbols", "special characters" and "punctuation marks" in password rules. Additionally, users are confused by partial lists of allowed characters using "e.g." or "etc."

Practical implications – This research provides data-driven usability guidance on constructing clearer language for password policies. Improving language clarity will help usability without sacrificing security, as simplifying password rule language does not change security requirements.

Originality/value – This is the first usable security study to systematically measure the effects of ambiguous password rules on user comprehension of the allowed character space.

Keywords Usability, Password policies, Password requirements, Password rule language, Usable security, User comprehension

Paper type Research paper

1. Introduction

> "No, they're not the same. A symbol is a symbol; it's not a letter and it's not a number. Special characters are not a symbol. It's like a punctuation mark. I'm sorry. Which ones are we talking about here?" (P07)

> "You could call it a symbol. I would call it a symbol. In the context of talking about passwords that would count as a symbol, I think. I'll think about it". (P46)

The authors gratefully acknowledge Dr I-Jeng Wang for his help with the expected capacity estimation and Dr Dan Wallach for his insightful comments.

Disclaimer. Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Information & Computer Security
Vol. 25 No. 1, 2017
pp. 80-99
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-06-2016-0043

> "Okay, well what's the difference between a symbol and a special character?" (P20)

> "I should know this, whether this is punctuation or whether it's a special character. That's where I got stumped, and I felt very embarrassed" (P43) (Anonymized participant reference codes are denoted as P##).

Users do not understand ambiguous language in password rules. Yet, passwords are still the most widely used authentication mechanism for controlling employees' access to organizational information systems. To protect data integrity and system security, organizations often establish enterprise-specific password policies dictating how employees should manage their organizational passwords. Those password policies are intended to ensure good password behaviors from users. However, across password policies, language can be inconsistent and ambiguous; terminology can be poorly defined.

Terms like "special characters" and "symbols" are confusing to users, as illustrated in the introductory quotes of this section. Users are often viewed by IT security professionals as the weakest link of cyber security (IT Governance, 2013; Haskins, 2007; Sasse *et al.*, 2001) and are frequently blamed for using insecure behaviors, such as selecting simple, easily guessed passwords. In response to users choosing predictable passwords, increasingly stringent and complex password policies have been imposed on users in an attempt to ensure system security. Such password requirements have also increased the visual and semantic complexity when presenting password rules to users, as shown in Figure 1.

As enterprise password policies can be quite lengthy and contain numerous password rules, rather than attempting to understand users' comprehension of an entire policy, we chose a more targeted approach focusing on individual password rules. This study investigates potentially ambiguous terminology in password rules and its effects on users' comprehension of the allowed character space. The results will ultimately serve to improve the usability of password policy language overall. Improving password policy language will

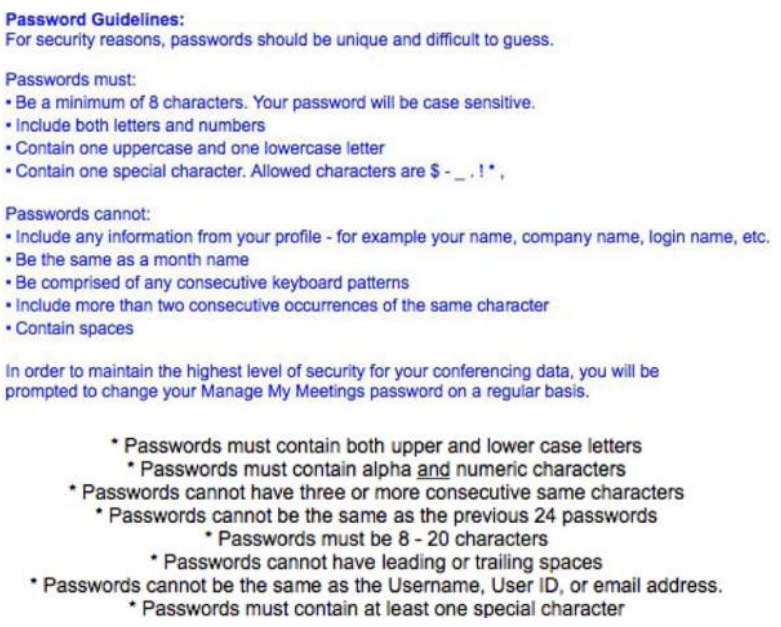


Figure 1.
Two anonymized screenshots of complex real-world password requirements, showing variability in language and formatting

help reduce user frustration, and allow users to more effectively generate compliant passwords.

The remainder of this paper is structured as follows: Section 2 describes the background and relevant literature. Section 3 details study methodology. Section 4 presents data and results. Section 5 discusses implications of study findings. Section 6 includes conclusions, limitations and future directions.

2. Literature review

Passwords are currently a good fit for many authentication needs, as passwords allow access from anywhere assuming only a simple browser, and revocation is as simple as changing passwords (Herley and van Oorschot, 2012). However, passwords pose numerous risks to security, such as vulnerability to attack (Bonneau, 2012; Kelley *et al.*, 2012; Weir *et al.*, 2009, 2010) and susceptibility to phishing via social engineering (Downs *et al.*, 2007; Mohebzada *et al.*, 2012; Nirmal *et al.*, 2015). To mitigate those vulnerabilities, organizations often utilize security measures such as imposing stringent password composition requirements, forcing password changes on a regular basis, preventing the use of prior passwords and providing employee security training and education. Furthermore, alternative authentication methods have been proposed, such as the use of biometrics, smart cards and various combinations of multiple methods for multi-factor authentication.

In addition to their security risks, passwords pose many usability issues as well. The user password management life cycle consists of three stages: generation, maintenance and authentication (Choong, 2014), each stage with its associated usability challenges. Password generation is, in essence, a complex problem-solving task including higher mental functions and creative thinking (Choong, 2014). The first step in password generation is to understand the constraints, in other words, to comprehend the problem space. Most password generation constraints consist of multiple individual rules that together define the allowable password contents. Individual password rules often include minimum length requirements and mandatory character classes (i.e. uppercase letters, lowercase letters, numbers and special characters). In sharp contrast to the abundance of prior research on password generation (von Zezschwitz *et al.*, 2013; Haque *et al.*, 2013; Campbell *et al.*, 2011; Brown *et al.*, 2004; Vu *et al.*, 2007; Florêncio and Herley, 2007; Florêncio *et al.*, 2014; Grawemeyer and Johnson, 2011; Furnell and Bar, 2013), research focusing on user comprehension of password rule terminology is unexpectedly limited. The current study is the first to begin addressing this research gap.

Despite the effort to bolster security with complex password requirements, there has been little corresponding effort to improve the language of user-facing password requirements. Improving language clarity will help usability without sacrificing security, as simplifying the language does not change the content of the security requirements. However, research is necessary to pinpoint which aspects of password requirements language are confusing to users. Although many aspects of passwords have been studied to date, there has been surprisingly little research on understanding users' comprehension of password rule language and specific terminology.

One very common password rule is the requirement for inclusion of "special characters". This is especially prevalent for enterprise-level and other high-value information systems. In contrast to unambiguous terms like uppercase letters (A-Z), lowercase letters (a-z) and numbers (0-9), definitions for the term *special characters* vary. For example, according to the Open Web Application Security Project, "Password special characters is an [*sic*] selection of punctuation characters that are present on standard USA keyboard and frequently used in passwords." (OWASP, 2016). In a different example, the Microsoft Windows 7 definition is

"A special character is a character that can't be found on your keyboard. You can insert special characters by using Character Map or by pressing a combination of keys on your keyboard." (Microsoft, 2016).

Terms like "special characters" and "symbols" are often used to refer to characters other than letters and numbers, i.e. non-alphanumeric characters. However, these terms are generally not explicitly defined in password policies. In a corpus of 40 real-world password policies, 24 referred to some concept of special characters, with 19 using the term "special characters", eight using "symbols", six using "punctuation" and two using "non-alphanumeric" (Steves *et al.*, 2014). Interestingly, several of these policies used multiple terms interchangeably. Only seven policies attempted to define the concept of special characters but gave incomplete lists of examples (most listed only two to four special characters).

Without explicit definitions, terms like "special characters" and "symbols" can be ambiguous to users, as users do not necessarily know exactly which characters are permissible in their passwords. As password generation tasks rely on users' comprehension of multiple complex password rules, ambiguity in any rule can negatively impact users during password rule comprehension. Therefore, understanding how users interpret and apply a single rule is a necessary first step to improving password rule language.

3. Methodology

While research on large-scale datasets (Das *et al.*, 2014; Weir *et al.*, 2010) offers quantitative insight regarding what constitutes user-generated passwords (e.g. character frequencies and arrangements), such studies do not necessarily offer explanations on why users choose certain character combinations in their passwords. Users' character selections are based on their comprehension of the allowed character space as specified in the password rules. Qualitative methods are best suited to investigate users' password rule comprehension by providing a deeper understanding of their thought processes. Qualitative methods and quantitative approaches complement one another and together provide more holistic and powerful insights.

We use a combination of quantitative and qualitative methods in a laboratory usable security study investigating user comprehension of confusing terminology in password rules. These methods allow us to provide data-driven usability guidance on constructing clearer language for password policies.

3.1 Participants

Sixty participants were recruited from a metropolitan area in the USA. Participants ranged in age from 22 to 69 years old (mean = 42.53, SD = 13.68), with 32 male and 28 female participants. The participants had diverse educational backgrounds and occupations. All participants had experience with work-related passwords. Participants were compensated for their time. Participants' demographics are summarized in Table I. We obtained informed consent verbally from all participants, both to participate in the study and to have their debriefings audio-recorded. Each participant was assigned a reference code, which was used in place of any personal identifiable information. All data were recorded and stored anonymously using the participants' reference codes only. Three participants did not complete the study in its entirety. For those tasks that they did complete, their data were included for analysis. Participants' debriefing audio recordings were transcribed by a professional transcription service.

3.2 Study design and procedure

We constructed eight character-selection tasks that varied the terms referring to non-alphanumeric characters to explore users' interpretations of password rule language. Additionally, we developed four compliance-checking tasks to investigate how well users can apply their understanding of the allowed character space. Each of these 12 tasks contained a password rule based on real-world password requirements (Table II). In some cases, rules were slightly modified or created to test particular differences in language. A detailed mapping of original password requirement sources and study modifications is presented in Figure A1. The first seven character-selection rules contained varying terminology regarding non-alphanumeric characters. In contrast, the last character-selection rule dealt with alphanumeric characters. Character-selection tasks asked participants to

Table I. Participant demographics

Age range	(%)	Education	(%)	Computer experience	(%)
≤30	25.00	High school	5.00	Novice	0.00
31-40	23.34	Associates	8.33	Average	33.33
41-50	20.00	Bachelor	55.00	Advanced	40.00
51-60	18.33	Master	25.00	Expert	25.00
>60	13.33	Advanced degrees	6.67	(n/a)	1.67

Table II. Password rules used in study tasks

Character-selection tasks Rule name	Password rule	Compliance-checking tasks Password rule
Symbols	The password must contain symbols	The password must contain one or more special characters (!@#$%^&*–+= etc.)
Special characters	The password must contain special characters	Passwords to be examined: hy&67gBpptype NnasVv8888@s Family_Tree=Big30 sUnsh1ne. Day
Non-alphanumeric	The password must contain non-alphanumeric characters	The password must contain one special character. Allowed characters are $-_.!*,
Special non-alphanumeric, e.g.	The password must contain special non-alphanumeric characters (e.g., ! @ # $ % ^ * ( ) – = + [ ] { } ; : ' ", . | / ? ~ \ )	Passwords to be examined: Submarine1$Ayoade Orchid4567!! El Chavo 12345! j*hUY63%ncjLD
Special non-alphanumeric, prohibited	The password must contain special non-alphanumeric characters. The characters listed below are not allowed: ~ ` & < >	The password must not contain spaces but can contain special characters. The special characters that are allowed are: ~ ! @ # $ % ^ & * ( ) { } [ ] | < > ? + – _ = / ; : '
Punctuation marks	The password must contain punctuation marks	Passwords to be examined: Bvy3T(8ghtTv fred4hetDdd 88Bluebeetle$$ am!4PaGen?\\
Punctuation, mathematical, conventional symbols	The password must contain punctuation marks, mathematical and other conventional symbols	The password can contain only numbers (0-9), upper and lower case letters (A-Z, a-z), hyphens (-), underscore (_) and periods (.) and the @ character
Alphanumeric	The password must contain alphanumeric characters	Passwords to be examined: Maroon5FTW-AA Kb9824.froPl French_onion12! (P1Gr02sterC

select all characters that met the rule from a character map (Figure 2), listing the 95 total characters (94 printable characters plus white space) available on a standard US keyboard: 26 uppercase letters, 26 lowercase letters, 10 numbers and the remaining 33 characters (referred to as non-alphanumeric characters hereafter). Each compliance-checking task asked participants to examine four passwords and an associated rule to determine whether each password met or did not meet the password rule. If participants decided a password did not meet the rule, they had to enter an explanation in a text field (Figure 3). Participants were presented one task at a time on a computer screen. Task presentation sequence and password order were randomized. Throughout the study, passwords were presented in Consolas font to visually distinguish easily confusable characters, e.g. number 0 versus uppercase letter O. Following completion of the tasks, participants were verbally debriefed.

4. Results

4.1 Character-selection tasks

Figure 4 shows selection percentages of the 33 non-alphanumeric characters for the character-selection tasks. Figure 4 arranges results based on the frequency of selection. In Figure 4, darker shading represents characters selected by over 90 per cent of the participants. Lighter shading represents characters selected by over 80 per cent of the participants.

Although terms like "symbols", "special characters" and "non-alphanumeric characters" seem to be used interchangeably in many password policies, our data show that participants did not interpret those terms as meaning the same thing. Depending on the exact terms used, participants' interpretations varied regarding what characters were allowed. In Figure 4, when the term "symbols" was used (first column), only eight characters were selected by more than 80 per cent of the participants. When the term "special characters" was used (second column), 25 characters were selected by more than 80 per cent of the participants. In contrast, for the "non-alphanumeric" rule (third column), all 32 non-alphanumeric characters except for white space were selected by more than 80 per cent of the participants. For the "non-alphanumeric" rule, the selection percentages were more uniformly distributed in

Figure 2.
Example of a character-selection task

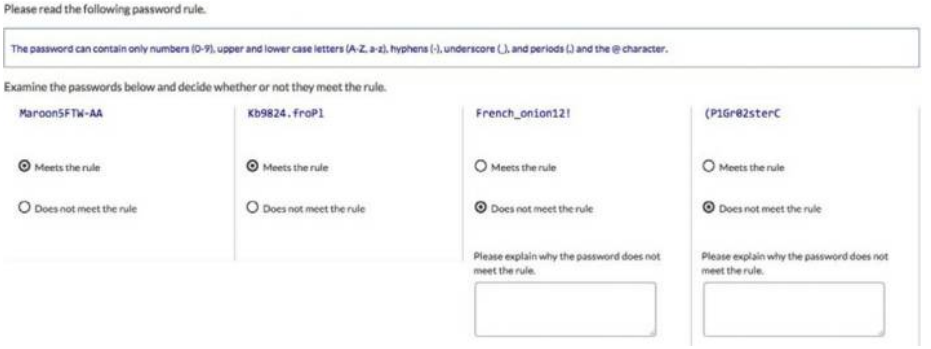


Figure 3.
Example of a compliance-checking task

Symbols		Special characters		Special non-alphanumeric, e.g.		Special non-alphanumeric, prohibited		Non-alphanumeric		Punctuation marks		Punctuation, mathematical, conventional symbols	
$	94.64%	#	98.18%	#	96.43%	!	92.59%	~	87.50%	.	98.25%	%	98.18%
%	94.64%	$	96.36%	$	96.43%	$	90.74%	!	87.50%	,	91.23%	.	98.18%
*	94.64%	^	96.36%	%	96.43%	%	90.74%	^	87.50%	!	89.47%	+	96.36%
@	92.86%	@	94.55%	^	96.43%	*	90.74%	*	87.50%	;	89.47%	!	94.55%
&	92.86%	%	94.55%	*	96.43%	#	88.89%	-	87.50%	:	89.47%	-	94.55%
#	89.29%	&	94.55%	(	94.64%	@	87.04%	`	85.71%	?	84.21%	=	94.55%
^	85.71%	*	94.55%	)	94.64%	^	87.04%	@	85.71%	'	80.70%	,	94.55%
~	80.36%	~	92.73%	+	94.64%	_	85.19%	#	85.71%	"	80.70%	?	94.55%
+	78.57%	(	89.09%	=	94.64%	(	83.33%	$	85.71%	`	38.60%	*	92.73%
>	78.57%	{	89.09%	[	94.64%	)	83.33%	%	85.71%	-	36.84%	;	92.73%
<	75.00%	}	89.09%	]	94.64%	-	83.33%	&	85.71%	(	35.09%	:	92.73%
`	73.21%	`	87.27%	!	92.86%	+	83.33%	(	85.71%	)	35.09%	$	90.91%
=	73.21%	)	87.27%	@	92.86%	=	83.33%	)	85.71%	~	24.56%	&	90.91%
[	73.21%	_	87.27%	-	92.86%	;	83.33%	_	85.71%	&	22.81%	/	89.09%
}	73.21%	+	87.27%	{	92.86%	"	83.33%	+	85.71%	{	22.81%	<	89.09%
!	71.43%	/	87.27%	}	92.86%	,	83.33%	=	85.71%	}	22.81%	>	89.09%
]	71.43%	<	87.27%	/	92.86%	.	83.33%	[	85.71%	/	22.81%	#	87.27%
\	71.43%	>	87.27%	|	91.07%	[	81.48%	]	85.71%	[	21.05%	'	87.27%
{	71.43%	!	85.45%	;	91.07%	]	81.48%	{	85.71%	]	21.05%	"	87.27%
|	71.43%	-	85.45%	:	91.07%	\	81.48%	}	85.71%	\	19.30%	(	85.45%
/	71.43%	=	85.45%	?	91.07%	{	81.48%	|	85.71%	<	17.54%	)	85.45%
(	69.64%	[	85.45%	~	89.29%	}	81.48%	.	85.71%	>	17.54%	[	83.64%
)	69.64%	]	85.45%	'	87.50%	|	81.48%	/	85.71%	^	15.79%	]	83.64%
?	69.64%	|	83.64%	,	87.50%	:	81.48%	<	85.71%	*	15.79%	{	81.82%
-	67.86%	\	81.82%	.	87.50%	/	81.48%	?	85.71%	_	14.04%	}	81.82%
_	64.29%	?	78.18%	"	83.93%	'	79.63%	\	83.93%	|	14.04%	_	80.00%
"	62.50%	"	76.36%	\	80.36%	?	79.63%	;	83.93%	@	12.28%	\	80.00%
;	60.71%	,	76.36%	_	78.57%	(ws)	11.11%	:	83.93%	+	12.28%	@	78.18%
:	60.71%	;	74.55%	<	76.79%	~	11.11%	'	83.93%	=	12.28%	^	78.18%
'	58.93%	:	74.55%	>	76.79%	`	9.26%	"	83.93%	#	10.53%	`	74.55%
,	58.93%	.	74.55%	&	75.00%	&	7.41%	,	83.93%	$	10.53%	~	72.73%
.	58.93%	'	72.73%	`	73.21%	<	5.56%	>	83.93%	%	10.53%	|	72.73%
(ws)	1.79%	(ws)	1.82%	(ws)	7.14%	>	3.70%	(ws)	25.00%	(ws)	5.26%	(ws)	1.82%

Notes: Percentages are ordered by frequency; the term "white space" is abbreviated as (ws)

Figure 4.
Selection percentages for non-alphanumeric characters, by password rule

comparison to the other five rules. These data show that terminology used in password rules can shrink or expand participants' selection of allowed characters.

In the "special non-alphanumeric, e.g." rule, 27 of the 33 non-alphanumeric characters were listed; only the hyphen, less-than sign, greater-than sign, ampersand, grave accent (- < > & `) and white space were not listed (Table II). Interestingly, simply listing characters increased participants' selection percentages for those characters (in comparison to rules where characters were not explicitly listed), as can be seen in the fourth column of Figure 4. As "e.g." is an abbreviation for the Latin phrase *exempli gratia*, meaning "for example", all non-alphanumeric characters were allowed in that rule. However, not all participants correctly interpreted the "e.g." as meaning "for example". Based on participants' comments in debriefings, it was clear that even if participants noticed "e.g.", they did not necessarily understand its meaning. Participants made comments such as "e.g. meaning just these" (P31), "I always forget the difference between i.e. and e.g." (P37) and "the e.g. is for exactly" (P53).

In the "special non-alphanumeric, prohibited" rule, five non-alphanumeric characters were explicitly prohibited: the tilde, grave accent, ampersand, less-than sign and greater-than sign (~ ` & < >), as specified in Table II. By explicitly listing prohibited characters, it helped participants to better understand the allowed character space, as shown in the fifth column of Figure 4. Participants' selection percentages for those five prohibited

non-alphanumeric characters were lower than 12 per cent, whereas participants' selection percentages for the allowed characters were all above or close to 80 per cent.

As seen in the sixth column of Figure 4, using the term "punctuation marks" further limited participants' character selection. There was a drastic drop (more than 40 per cent) in selection percentages between the top eight characters and the remaining characters. Participants seemed to view punctuation as only referring to characters used in writing. For example, P31 stated, "Punctuation marks only mean the marks that I would use to punctuate a sentence.". P53 commented, "anything that I've seen while writing or used in a sentence, to like edit and stuff". Furthermore, participants viewed punctuation as a very narrow subset of all non-alphanumeric characters. P30 said, "When I see symbols, I leave out punctuation marks.". P33 stated, "Punctuation means something different than special characters.". However, when the terminology was "punctuation, mathematical, and other conventional symbols" (seventh column of Figure 4), participants' selections became more expansive.

Participants expressed confusion and uncertainty about the meaning of the various terms for non-alphanumeric characters. P03 noted, "I always consider like everything that's not the alphabet or a number to be a special character, but it might not be.". P12 expressed doubt, "I was like, wait. Am I considering these all under one bubble? Am I really separating them?". Similarly, P20 said, "Okay, well what's the difference between a symbol and a special character?". P42 noted, "It is very confusing when it says special characters or symbols.". P55 commented, "I was wondering if for example punctuation, does that mean the same as special characters?". Some participants used the keyboard to illustrate their interpretations of special characters. P20 said, "I'm thinking of the SHIFT on the top bar for the most part.". P39 stated, "I finally decided that special characters must be these on the very top. That was my conclusion. Whether it's right or not, I don't know.".

Some participants seemed to conceptualize terms as hierarchical: P39 said, "Special characters I would think of as being a little bit more limited, and symbols being a little bit more broad", and P51 noted, "Non-alphanumeric seemed to be a larger group, and then things like symbols or equation became subsets of that group, so it would limit it more, in my head anyway.". In contrast, others thought "special characters" and "symbols" were synonymous: "I thought special characters and symbols are the same. That's the way I interpret it" (P42), and "Special characters and symbols I pretty much lumped together as one and the same" (P59).

Although white space is a non-alphanumeric character – not a letter and not a number – only 25.00 per cent of the participants considered it as such in the "non-alphanumeric" rule (Figure 4, third column). Selection percentages for white space across other rules were much lower, 1.79 per cent to 7.14 per cent. Participants were confused about white space: P09 said, "I always have been confused because I don't know if it's a special character. I don't consider it a special character, but I do consider it a non-alphanumeric character. I would just specifically state that spaces are or are not allowed", and P58 noted, "I think that was a little confusing, as to where the space fell into. I wasn't certain if that was a special character or not.".

In password requirements, the term "non-alphanumeric" often refers to characters other than letters and numbers. However, for the "non-alphanumeric" rule, over 17 per cent of the participants incorrectly selected letters (17.86 per cent for uppercase and 17.31 per cent for lowercase), and 14.29 per cent of the participants incorrectly selected numbers. For the "alphanumeric" rule, nearly a quarter of the participants failed to select letters (23.21 per cent for both uppercase and lowercase), and 10.71 per cent failed to select numbers. Participants expressed uncertainty regarding alphanumeric and non-alphanumeric: P12 said, "So I think the non-alphanumeric was most vague to me. I was like, so it can really be any of these that

aren't just numbers or letters?", and P25 noted, "Non-alphanumeric was like does that mean anything that's not a number? That's what I thought.".

4.1.1 Estimate of the expected capacity of password rules for non-alphanumeric characters. Expected capacity measures the average "size" of the space of possible password patterns generated by the user population following a set of rules. We can estimate the expected capacity of those password rules with varying terminology specifying non-alphanumeric characters. This is important because people's interpretations of password rules vary, which affects their potential allowable non-alphanumeric character space.

Let $W = (X_1, X_2, \ldots, X_N)$ be a compliant password of length N, where X_n's are from a finite character set $A = \{a_1, \ldots, a_M\}$. Assume that W is modeled statistically as follows:

- X_n's are independent and identically distributed.
- Each character a_m in A may be included (or considered) for selection with probability $1 \geq q_m \geq 0$. We assume independent inclusion across the characters. That is, whether a character is included has nothing to do with whether any others are included. We will use a binary random variable $S_m \in \{0,1\}$ to denote whether the character a_m is included. Hence, $P\{S_m = 1\} = q_m$.

Define the expected capacity of W, $C_N(W)$, as the expected number of possible distinct passwords following the model described above. Then, with the independent assumptions, $C_N(W)$ can be derived as:

$$C_N(W) = \left[E\left(\sum_{m=1}^{M} S_m\right)\right]^N = \left[\sum_{m=1}^{M} q_m\right]^N$$

Here we are only examining the expected capacity in a single position of any possible password. Thus, we will use $C_1(W) = \sum_{m=1}^{M} q_m$ to denote the expected capacity of a word with length one.

To estimate each inclusion probability q_m from data, one will collect n independent samples of S_m. That is, one will survey n subjects to determine whether the character a_m is included for selection. Let L_m denote the number of subjects who respond positively to include character a_m. Then it is clear that the simple estimate $\hat{q}_m = L_m/n$ is an unbiased estimate of S_m and that L_m follows the binomial distribution.

In this study, the finite character set A contains the 33 non-alphanumeric characters (as described in the Methodology section). Thus, the maximum expected capacity of the non-alphanumeric characters is 33, if all 33 characters are included for selection with probability 1. Using the data in Figure 4, $\hat{q}_m$ is the selection percentage of each non-alphanumeric character. For each password rule, we calculate the estimated $C_1(W)$, as shown in Table III. It is clear that none of the rules has achieved the maximum expected

Table III.
Expected capacity of password rules for character-selection tasks

Rule name	Expected capacity
Symbols	$C_1(W) = 23.82$
Special characters	$C_1(W) = 27.62$
Non-alphanumeric	$C_1(W) = 27.64$
Special non-alphanumeric, e.g.	$C_1(W) = 28.75$
Special non-alphanumeric, prohibited	$C_1(W) = 23.22$
Punctuation marks	$C_1(W) = 11.95$
Punctuation, mathematical, conventional symbols	$C_1(W) = 27.95$

capacity of 33. The rule with expected capacity closest to the maximum is the "Special non-alphanumeric, e.g." rule, with expected capacity of 28.75, about 87.12 per cent of the maximum capacity. The rule with the lowest expected capacity is the "Punctuation marks" rule, with expected capacity of 11.95, about 36.21 per cent of the maximum capacity. Empirically, we observe variability of expected capacity among different password rules. However, to be able to perform statistical testing among rules, we will need to increase our sample size in the future to permit normal approximation.

4.2 Compliance-checking tasks

Four password rules were used in the compliance-checking tasks. As shown in Table II, each rule contained four passwords to be examined for compliance by the participants. For each password rule, the researchers carefully selected passwords as stimuli to be compliant or non-compliant. Participants' answers were counted as errors if participants marked the passwords incorrectly, for example marking a compliant password as non-compliant and vice versa. Table IV shows the error rate for each password.

4.2.1 Rule – must contain one or more special characters: partial list of 11 with "etc.". For this rule, two passwords (NnasVv8888@s and hy&67gBpptype) contained special characters explicitly listed in the rule, whereas the other two passwords (Family_Tree=Big30 and sUnsh1ne.Day) contained special characters not listed, but still implicitly permissible due to the use of "etc." in the rule. All four passwords met the rule (Table IV). The passwords with explicitly allowed special characters had lower error rates than those with implicitly allowed special characters. Although there were two special characters in the Family_Tree=Big30 password, only the equals to sign was explicitly listed in the password rule. The underscore was not listed, but because of the "etc.", it was a permissible special character. As shown in Table IV, the password Family_Tree=Big30 had an error rate of 13.56 per cent. The most difficult password for participants was sUnsh1ne.Day. Although the period was not listed in the rule, it was still a permissible special character. The error rate for sUnsh1ne.Day was 61.02 per cent, over four times higher than that for the password Family_Tree=Big30. Either participants did not notice or did not

Rule description	Password	Compliant with rule?	Participant error rate (%)
Must contain one or more special characters: partial list of 11 with "etc."	NnasVv8888@s	Yes	5.08
	hy&67gBpptype	Yes	8.47
	Family_Tree=Big30	Yes	13.56
	sUnsh1ne.Day	Yes	61.02
Must contain one special character: list of 7 allowed	Submarine1$Ayoade	Yes	1.72
	Orchid4567!!	Yes	37.93
	j*hUY63%ncjLD	No	43.10
	El Chavo 12345!	No	82.76
Can contain special characters: list of 27 allowed	88Bluebeetle$$	Yes	8.62
	Bvy3T(8ghtTv	Yes	18.97
	fred4hetDdd	Yes	20.69
	am!4PaGen?\\	No	29.31
Can contain only numbers, letters, hyphens (-), underscore (_) and periods (.) and the @ character	Maroon5FTW-AA	Yes	10.00
	Kb9824.froPl	Yes	10.00
	French_onion12!	No	11.67
	(P1Gr02sterC	No	18.33

Table IV. Compliance-checking participant error rates

understand the use of "etc.". Of those who incorrectly marked sUnsh1ne.Day as not meeting the rule, 91.67 per cent referred to a lack of special characters in their explanations. Participants gave explanations such as "does not contain one of the listed special characters" (P03) and "no special characters – just a period – this is not one of the allowable characters" (P05). P29 typed, "The period is not really a special character, meaning you do not have to push SHIFT to access it from the keyboard." P49 entered, "I'm pretty sure regular punctuation is not considered a special character."

4.2.2 Rule – must contain one special character: list of seven allowed. For this rule, two passwords (Submarine1$Ayoade and Orchid4567!!) were compliant, as they contained one of the allowed special characters listed in the rule. The password j*hUY63%ncjLD was not compliant because it contained the percentage sign, which was not listed as an allowed special character. Although the password El Chavo 12,345! contained the allowed exclamation mark, it contained two white spaces. White space was not specified as an allowed special character in the rule. Across passwords, the error rates were high, ranging from 37.93 per cent to 82.76 per cent, except for the password Submarine1$Ayoade, which only one participant incorrectly marked as non-compliant, as shown in Table IV.

For the compliant password Orchid4567!!, 37.93 per cent of the participants incorrectly marked it as non-compliant. Of those who incorrectly marked the password as non-compliant, an overwhelmingly high percentage of participants (95.45 per cent) gave the same reason, that there were two special characters in the password. Participants interpreted the language "[…] must contain one special character" in the password rule as meaning literally "only one" special character was allowed: P03 explained, "contains more than one special character from the list", and P41 typed, "the password must contain one special character not more".

For the non-compliant password j*hUY63%ncjLD, 43.10 per cent of the participants failed to recognize that the percentage sign was not among the allowed characters listed and incorrectly marked the password as compliant. Although more than half of the participants correctly marked the password as non-compliant, we found that the participants did not necessarily understand the rule completely. Out of those who made the correct determination, 18.18 per cent gave wrong explanations for the non-compliancy, often implying that only one special character was allowed. For example, P08 typed, "% not allowed more then [*sic*] one special chara [*sic*] included"; P39 entered, "password contains 2 special characters"; and P44 explained, "Has more than one special character".

For the other non-compliant El Chavo 12,345! password, only 17.24 per cent of the participants correctly marked it as non-compliant. The majority of participants (82.76 per cent) failed to recognize that white space was not specified as an allowed special character in the rule. This can be attributed to the fact that many participants did not consider the white space as a special character.

4.2.3 Rule – can contain special characters: list of 27 allowed. This rule was particularly interesting due to the language "[…] can contain special characters", which implies that special characters are allowed but not required. However, if a password does contain any special characters, they must be from the allowed list. For this rule, three passwords were compliant and one was non-compliant. The error rate for the compliant 88Bluebeetle$$ password was fairly low, only 8.62 per cent, in Table IV. Most participants correctly marked the password 88Bluebeetle$$ as compliant, with relatively few participants incorrectly marking it as non-compliant. Interestingly, several participants referred to the style of the dollar signs in their explanations for why they marked the password 88Bluebeetle$$ as non-compliant. For example, P05 explained, "The letters at the end are not dollar signs, but the letter S with a strike through"; P39 typed, "$ sign doesn't match the rule. It is italicized"; and P52 entered, "The two symbols at the end are not standard dollar signs – this is not allowed."

The 18.97 per cent error rate for the compliant password Bvy3T(8ghtTv was over twice as high as that for the 88Bluebeetle$$ password. Of those participants who incorrectly marked the password Bvy3T(8ghtTv as non-compliant, most participants (81.82 per cent) explained that there were spaces in the password, which were prohibited by the password rule. However, there were no spaces in the password. Several other participants referred to a lack of special characters, which implies that they may have simply missed the parenthesis embedded in the middle of the password.

The error rate for the compliant password fred4hetDdd was 20.69 per cent, very similar to that of the Bvy3T(8ghtTv password. Of those participants who incorrectly marked the password fred4hetDdd as non-compliant, the majority of participants (91.67 per cent) described their reasoning as due to a lack of special characters in the password. This implies that participants misinterpreted the "can contain special characters" as "must contain special characters" in the password rule. Having an explicit list of allowed special characters may have reinforced this misinterpretation of the word "can" for "must". P16 explained, "Has to include a special character", and P31 typed, "Does not contain any of the special characters specified".

The error rate for the non-compliant password am!4PaGen?\\ was the highest of the four passwords, at 29.31 per cent. Due to the presence of the backslashes, which were not allowed special characters, the password was non-compliant. Although the backslash was not in the list of allowed special characters, the forward slash was. For those participants who incorrectly marked the password as compliant, it is possible they confused those two characters. Interestingly, some participants who correctly marked the password as non-compliant actually gave the wrong reason; 9.76 per cent of those participants referred to white spaces in their explanations.

4.2.4 Rule – can contain only numbers, letters, hyphens (-), underscore (_) and periods (.) and the @ character. Similar to the Chk_Can rule, this Chk_Can.limit rule also used "can" rather than "must". However, in this Chk_Can.limit rule, the allowed special characters were limited to only four characters: the hyphen, underscore, period and at sign (- _ . @). Similar to the Chk_Can rule, if a password does contain any special characters, they must be from the allowed list. For this Chk_Can.limit rule, two passwords were compliant and two were non-compliant.

As shown in Table IV, error rates for the two compliant passwords, Maroon5FTW-AA and Kb9824.froPl, were both 10.00 per cent. The reasons participants gave for incorrectly marking them as non-compliant were similar across the two passwords. Participants thought that all four of the listed special characters were required. Although the password rule listed four allowed special characters, nowhere did it say that all four characters must be contained in the password. Regarding the password Maroon5FTW-AA, P01 explained, "It has numbers, lower case letters, a hyphen but no underscore, period and @ character.". P15 typed, "Password does not contain @ . _". Explanations were similar regarding the Kb9824.froPl password. For example, P01 explained, "Does not contain the @ character, underscore or hyphen". P07 entered, "no: _@".

Due to the inclusion of an exclamation mark, which was not an allowed special character, the password French_onion12! was non-compliant. However, 11.67 per cent of the participants incorrectly marked it as compliant, an error rate similar to that of the two compliant passwords. More interestingly, 11.32 per cent of the participants who correctly marked the password as non-compliant actually gave erroneous explanations for their responses. A few participants again thought that all the four special characters were required. For example, P07 typed, "no -, @". P15 explained, "The password is missing hyphens, periods and @ character.". Other erroneous explanations referred to the number 12, with participants misinterpreting the "[…] only numbers (0-9)" requirement in the password

rule. For instance, P31 entered, "Contains the numer12 [*sic*]". P15 explained, "Password has a 12 in it. Numbers are only between 0-9.".

The (P1Gr02sterC password was non-compliant due to the inclusion of the left parenthesis, which was not an allowed special character. However, 18.33 per cent of the participants incorrectly marked the (P1Gr02sterC password as compliant, an error rate noticeably higher than that of the non-compliant French_onion12! password. Again, 14.29 per cent of the participants who correctly marked the (P1Gr02sterC password as non-compliant actually gave erroneous explanations for their responses. As with the other passwords, participants thought that all the four special characters were required. P01 typed, "doens't [*sic*] have the @, underscore or period". P07 entered, "no: @.@_". P15 explained, "Password is missing @character and underscore".

5. Discussion

People are sensitive to nuances in language. In our study, different password rule terminologies elicited different reactions and interpretations from the participants. Here we discuss key findings with supporting evidence.

5.1 Are there differences between symbols, special characters and punctuation marks?

People are not sure. Our data show great variability and confusion in participants' understanding of these three terms. Participants made comments such as "for the symbols, I didn't know exactly what you meant" (P29) and "it was kind of a little bit hard to differentiate between special character and symbol" (P32). Some participants thought the terms meant the same thing, with comments like "I thought symbol meant the special characters more than anything." (P37) and "I'm assuming that the symbols and the special characters would be synonymous. They might not be, but that's my assumption." (P57). When participants described these three terms in their own words, several interesting themes emerged, as described below:

(1) *Special characters*: Use of the modifier "special" impacted how participants defined allowed characters. Participants had different definitions of the modifier "special" in the context of special characters. Some defined it based on the frequency of use, "Special characters like we don't use it all the time – not as common" (P26). Others defined it in terms of requiring an extra action to execute, "anything you have to use a SHIFT key" (P41).

(2) *Symbols*: Some participants interpreted "symbols" as referring to those characters representing concepts. For instance, the dollar sign ($) represents money, and the number sign (#) represents numbers. Participants gave examples such as "Well symbol means, to me, it's a dollar sign. That means money. A symbol means the at sign – at something." (P28), and "Symbols meant the things that meant something, like the number is a symbol for number" (P55).

(3) *Punctuation*: Participants viewed punctuation as a class of its own, something very distinct from special characters and symbols, "No, they [referring to special characters and symbols] kind of meant the same thing. But they still excluded, for me, punctuation marks." (P60). Participants gave descriptions of punctuation that were very narrow in scope, limited to only those characters used in writing, such as "I kind of consider punctuation marks to be a character at the end of the sentence." (P09); "When you write a sentence. Yeah. You use punctuation marks." (P28); and "punctuation marks I know, whatever, at the end of a sentence or in the middle of a sentence" (P42).

5.2 Expected capacity of password rules varies based on rule language

As previously described, the maximum expected capacity of the non-alphanumeric characters is 33, if all 33 characters are included for selection with probability of 1. However, none of the password rules examined in this study achieved the maximum expected capacity. Depending on the terminology used in the password rules, the expected capacity ranged from approximately 36 per cent (for the "Punctuation marks" rule) to 87 per cent (for the "Special non-alphanumeric, e.g." rule) of the theoretical maximum expected capacity.

5.3 Users often take password rule language literally

Across compliance-checking tasks, there were multiple examples of participants interpreting password rules quite literally. Participants literally interpreted "one" as singular, meaning "one and only one". This contrasts with the password rule's implied intention of requiring a minimum of one special character. Several participants were also extremely literal in their interpretation of "numbers (0-9)". They interpreted this to mean single digit numbers between zero and nine. For example, participants viewed the number "12" in the password French_onion12! as a single entity, rather than being composed of two digits "1" and "2".

In addition to overly literal interpretations of password rules, participants simply misunderstood certain words: "can" and "must". In the context of password rules, the use of "can" implies that listed characters are optional, whereas "must" means that they are required. However, participants interpreted "can contain" as meaning "must contain". From a linguistic perspective, this does not make sense because "can" and "must" are clearly distinct: "can" gives permission, while "must" mandates. Yet, given participants' past experience with passwords requirements, which usually include "must" statements, perhaps their interchangeable interpretation of "can" and "must" was not so unreasonable. Using the single word "can" clearly is not sufficient to convey the concept of optional inclusion to users. If certain characters are truly not required, that optionality should be made clear to users.

5.4 Technical terms like "non-alphanumeric" are confusing to users

Terms that may be common in the security community, such as "non-alphanumeric", are not necessarily understood by all users. Even though participants in our study had enterprise password experience, the terms "non-alphanumeric" and "alphanumeric" still posed difficulty for them, with comments like "The alphanumeric characters and the non-alphanumeric characters, the symbols. That was like kind of confusing, to be honest, you know. I wasn't exactly sure what they were referring to at times." (P34), and "I think non-alphanumeric and alphanumeric I guess could be confusing." (P58). Technical terms like "non-alphanumeric" and "alphanumeric" should be clearly defined. This is most critical with "non-alphanumeric" because permissible characters can vary widely from system to system. However, the term "alphanumeric" should also be defined so users understand that it refers to both letters and numbers (an exhaustive list of allowed letters and numbers should not be necessary, as all letters and numbers are usually allowed).

5.5 Explicitly listing allowed non-alphanumeric characters benefits users, if done carefully

Listing allowed non-alphanumeric characters increased participants' selection percentages for those characters. Participants appreciated having examples listed, with comments like "You can't just say special characters, you need to give examples." (P38), and "I think having the examples, and if it contained all of the examples, they are pretty good." (P58). However,

our results also show that participants did not understand "etc." in the compliance-checking task, nor did they understand "e.g." in the character-selection task. Together, these results show that if a password policy lists permissible special characters, it should list all the permissible special characters. If certain characters are to be prohibited, they should be explicitly specified as well.

5.6 White space is not widely considered a non-alphanumeric character

White space was a source of confusion for participants across the character-selection and compliance-checking tasks. In addition to being confused about whether white space was a non-alphanumeric character, participants also made comments like "I never considered a blank space to be a character." (P03); "For me, I would never use spaces." (P23); "I'm like, I don't see anything." (P29); "Wow, I never used the space bar in my thing. What is the space bar considered? Is it a character? Is it not a character? Is it just a space?" (P51); and "One thing I was confused about is white space. I never considered that. I never think about that in terms of using it within a password." (P55). Password requirements should be explicit regarding whether they allow or prohibit white space.

6. Conclusions and future directions

This user research provides important data-driven guidance on constructing clearer language for password policies. Terminology used in password rules can have unintended consequences on users' understanding of the allowed versus prohibited character space. By combining qualitative and quantitative research methods in our study, we discovered substantial effects of varying terminology in the context of password rule comprehension. Seemingly small changes in language have large, observable impacts on users' understanding of password rules and affect the expected capacity of the password rules. Depending upon the exact terms used – special characters, symbols, punctuation marks or non-alphanumeric characters – users' interpretation of the allowed character space can shrink or expand. Therefore, it is critical that password requirements avoid ambiguous terminology. This can be accomplished by avoiding jargon words such as "non-alphanumeric" unless they are explicitly defined. Furthermore, rather than giving a partial list with "e.g." or "etc.", an exhaustive list of allowed non-alphanumeric characters should be defined for users.

Password rules are often constructed to be sentence-like by combining verbs and objects, for example "must include special characters", "can contain a symbol", "cannot use punctuation marks", "must contain numerals" or "can contain numbers 0-9". We found that users can interpret password rule language in unintended and surprising ways. As in any domain, clear and concise language can help increase task success and reduce user frustration. To evaluate effects of improving password rule language, a two-phase approach is necessary: identify problematic language and suggest improvements, and validate the efficacy of suggested improvements. The current study was intended only to address the first phase, with future research planned to address the second phase. Thus, a limitation of the current study is that it did not evaluate the effects of suggested language improvements. For example, does improving language clarity measurably increase task success and reduce user frustration? Does improving language clarity lead to stronger, more variable passwords? Password rule language must be carefully constructed and tested with representative users to ensure that users fully comprehend the rules as intended, and can generate compliant passwords. Password rules will never achieve their maximum security potential if end-users perceive the allowed character space as smaller than the intended character space.

Although the current study was focused on terminology for non-alphanumeric characters commonly found in password generation rules, the issue of language clarity applies to password management policies in their entirety as well. In addition to password generation requirements, password management policies often include requirements for password expiration, reuse, storage, etc. Policy makers should use terminology that is appropriate for the target audience (e.g. end-users, system administrators, developers, policy implementers). In addition to benefiting end-users, language clarity will also help those who must implement the password policies to ensure that policies are implemented as intended. Only after sources of confusion have been identified, can solutions be evaluated to fix the ambiguity in password rule language. Future research should expand upon the terminology and rules examined and replicate with different user populations beyond end-users, such as system administrators, policy implementers and security experts.

References

Bonneau, J. (2012), "The science of guessing: analyzing an anonymized corpus of 70 million passwords", *Proceedings of the 2012 IEEE Symposium on Security and Privacy, IEEE Computer Society, San Francisco, CA*, pp. 538-552.

Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. (2004), "Generating and remembering passwords", *Applied Cognitive Psychology*, Vol. 18, pp. 641-651.

Campbell, J., Ma, W. and Kleeman, D. (2011), "Impact of restrictive composition policy on user password choices", *Behaviour and Information Technology*, Vol. 30 No. 3, pp. 379-388.

Choong, Y.-Y. (2014), "A cognitive-behavioral framework of user password management lifecycle", *Human Aspects of Information Security, Privacy, and Trust*, pp. 127-137.

Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X. (2014), "The tangled web of password reuse", *Network and Distributed System Security Symposium (NDSS'14)*.

Downs, J.S., Holbrook, M. and Cranor, L.F. (2007), "Behavioral response to phishing risk", *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, ACM, New York, NY*, pp. 37-44.

Florêncio, D. and Herley, C. (2007), "A large-scale study of web password habits", *Proceedings of the 16th International Conference on World Wide Web, ACM, New York, NY*, pp. 657-666.

Florêncio, D., Herley, C. and Van Oorschot, P. (2014), "Password portfolios and the finite-effort user: sustainably managing large numbers of accounts", *Proceedings of USENIX Security, USENIX Association, San Diego, CA*, pp. 575-590.

Furnell, S. and Bar, N. (2013), "Essential lessons still not learned? Examining the password practices of end-users and service providers", *Human Aspects of Information Security, Privacy, and Trust*, pp. 217-225.

Grawemeyer, B. and Johnson, H. (2011), "Using and managing multiple passwords: a week to a view", *Interacting with Computers*, Vol. 23 No. 3, pp. 256-267.

Haque, S.M.T., Wright, M. and Scielzo, S. (2013), "A study of user password strategy for multiple accounts", *Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy, ACM, New York, NY*, pp. 173-176.

Haskins, W. (2007), "Network security: gullible users are the weakest link", *TechNewsWorld*, available at: www.technewsworld.com/story/60520.html (accessed May 2016).

Herley, C. and van Oorschot, P. (2012), "Research agenda acknowledging the persistence of passwords", *IEEE Security and Privacy*, pp. 28-36.

IT Governance (2013), *Boardroom Cyber Watch 2013: Report*.

Kelley, P.G., Komanduri, S., Mazurek, M.L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F. and Lopez, J. (2012), "Guess again (and again and again): Measuring password strength by

simulating password-cracking algorithms", *Proceedings of IEEE Symposium on Security and Privacy*, *IEEE Computer Society*, *San Francisco, CA*, pp. 523-537.

Microsoft (2016), "Using special characters (character map)", available at: http://windows.microsoft.com/en-us/windows/using-special-characters-character-map-faq-1TC=windows-7 (accessed May 2016).

Mohebzada, J.G., El Zarka, A., Bhojani, A.H. and Darwish, A. (2012), "Phishing in a university community: two large scale phishing experiments", *Innovations in Information Technology (IIT)*, pp. 249-254.

Nirmal, K., Janet, B. and Kumar, R. (2015), "Phishing - the threat that still exists", *2015 International Conference on Computing and Communications Technologies (ICCCT)*, *IEEE Computer Society*, *Chennai*, pp. 139-143.

Open Web Application Security Project (OWASP) (2016), "Password special characters", available at: www.owasp.org/index.php/Password_special_characters (accessed May 2016).

Sasse, M.A., Brostoff, B. and Weirich, D. (2001), "Transforming the 'weakest link' – a human/computer interaction approach to usable and effective security", *BT Technology Journal*, Vol. 19, pp. 122-131.

Steves, M., Killourhy, K. and Theofanos, M.F. (2014), "Clear, unambiguous password policies: an oxymoron?", *Cross-Cultural Design*, pp. 240-251.

von Zezschwitz, E., De Luca, A. and Hussmann, H. (2013), "Survival of the shortest- a retrospective analysis of influencing factors on password composition", *Human-Computer Interaction – INTERACT*, Springer Berlin Heidelberg, pp. 460-467.

Vu, K.P.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B.L., Cook, J. and Schultz, E.E. (2007), "Improving password security and memorability to protect personal and organizational information", *International Journal of Human-Computer Studies*, Vol. 65, pp. 744-757.

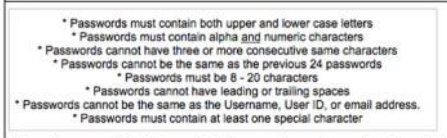
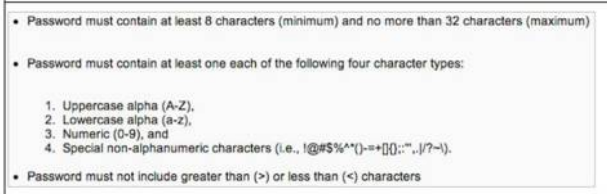
Weir, M., Aggarwal, S., De Medeiros, B. and Glodek, B. (2009), "Password cracking using probabilistic context-free grammars", *Proceedings of IEEE Symposium on Security and Privacy*, *IEEE Computer Society*, *Oakland, CA*, pp. 391-405.

Weir, M., Aggarwal, S., Collins, M. and Stern, H. (2010), "Testing metrics for password creation policies by attacking large sets of revealed passwords", *Proceedings of CCS*, *ACM (Association for Computing Machinery)*, *New York, NY*, Vol. 10, pp. 162-175.

Appendix

As the goal was to demonstrate variability across password requirements rather than single out any particular system, screenshots have been anonymized. Figure A1 maps rules used in this study to their original source material. In this study, a single rule was selected from each set of password requirements. In some cases, rules were slightly modified or created to test particular differences in password language, as described below in Figure A1.

Character-Selection Tasks

Rule Name	Password Rule and Partial Screen Shot of Source
Symbols	The password must contain symbols.  (Must be between 12 and 15 characters in length. Must contain at least 1 Number, 1 Uppercase Letter and 1 Symbol) This rule was modified: "1 Symbol" was changed to "symbols."
Special characters	The password must contain special characters.  * Passwords must contain both upper and lower case letters * Passwords must contain alpha and numeric characters * Passwords cannot have three or more consecutive same characters * Passwords cannot be the same as the previous 24 passwords * Passwords must be 8 - 20 characters * Passwords cannot have leading or trailing spaces * Passwords cannot be the same as the Username, User ID, or email address. * Passwords must contain at least one special character This rule was modified: "a special character" was changed to "special characters."
Non-alphanumeric	The password must contain non-alpha-numeric characters.  Enter a new password: The password must: • have at least 12 characters • have at least 1 non-alphanumeric characters • have at least 1 letters • have at least 1 digits • not contain a dictionary word (e.g. xyzw1o2r3d) • not be the profile ID or name • not be the profile ID or name backwards • not contain the profile ID or name • not contain your user name or any part of your full name • contain elements from three of the four following types of characters: English upper case letters, English lower case letters, Westernized Arabic numerals, non-alphanumeric character • contain only characters available on a standard English (US) keyboard. List of valid characters • not have 5 occurrences of the same character • not be an old password • allow old passwords after 730 days • maximum password age (required to change every 90 days) The password should: • not contain the profile ID or name backwards This rule was modified: "1 non-alphanumeric characters [*sic*]" was changed to "non-alpha-numeric characters."
Special non-alphanumeric, e.g.	The password must contain special non-alphanumeric characters (e.g., ! @ # $ % ^ * ( ) - = + [ ] { } ; : ' " , . | / ? ~ \ ).  • Password must contain at least 8 characters (minimum) and no more than 32 characters (maximum) • Password must contain at least one each of the following four character types: 1. Uppercase alpha (A-Z), 2. Lowercase alpha (a-z), 3. Numeric (0-9), and 4. Special non-alphanumeric characters (i.e., !@#$%^*()-=+[]{};:'",.|/?~\). • Password must not include greater than (>) or less than (<) characters This rule was modified: the "i.e." was changed to "e.g."
Special non-alphanumeric, prohibited	The password must contain special non-alphanumeric characters. The characters listed below are not allowed: ~ ` & < > This rule was created to investigate effects of a prohibited list.

(*continued*)

Figure A1.
Passwords rules and partial screenshots of sources

Punctuation, mathematical, conventional symbols	The password must contain punctuation marks, mathematical and other conventional symbols.
	Your password has expired. Passwords need to be a minimum of 8 characters. Password characters should be a combination of alphanumeric characters. Alphanumeric characters consist of letters, numbers, punctuation marks, mathematical and other conventional symbols.
Alphanumeric	The password must contain alpha-numeric characters.
	This rule was created to contrast the non-alphanumeric rule.
Compliance-Checking Tasks	
Rule Description	**Password Rule and Partial Screen Shot of Source**
Must contain one or more special characters: partial list of 11 with "etc"	The password must contain one or more special characters (!@#$%^&*-+= etc).
	Password restrictions: Must be at least eight characters and must meet at least **three** of the following: • One or more lowercase alphabetic characters (a-z) • One or more uppercase alphabetic characters (A-Z) • One or more numeric characters (0-9) • One or more special characters (!@#$%^&*-+= etc)
Must contain one special character: list of 7 allowed	The password must contain one special character. Allowed characters are $-_.!*,
	Password Guidelines: For security reasons, passwords should be unique and difficult to guess. Passwords must: • Be a minimum of 8 characters. Your password will be case sensitive. • Include both letters and numbers • Contain one uppercase and one lowercase letter • Contain one special character. Allowed characters are $ - _ . ! * , Passwords cannot: • Include any information from your profile - for example your name, company name, login name, etc. • Be the same as a month name • Be comprised of any consecutive keyboard patterns • Include more than two consecutive occurrences of the same character • Contain spaces In order to maintain the highest level of security for your conferencing data, you will be prompted to change your Manage My Meetings password on a regular basis.
Can contain special characters: list of 27 allowed	The password must not contain spaces but can contain special characters. The special characters that are allowed are: ~ ! @ # $ % ^ & * ( ) { } [ ] | < > ? + - _ = / ; : '
	Password Rules: • Must be a minimum of 8 characters and a maximum of 20 characters • Must not contain spaces but can contain special characters. The special characters that are allowed are: ~ ! @ # $ % ^ & * ( ) { } [ ] | < > ? + - _ = / ; : ' " , . ` • Must include at least one letter and at least one number • Must include at least one uppercase letter • Passwords are case sensitive
Can contain only numbers, letters, hyphens (-), underscore (_), and periods (.) and the @ character.	The password can contain only numbers (0-9), upper and lower case letters (A-Z, a-z), hyphens (-), underscore (_), and periods (.) and the @ character.
	What are the rules for specifying a password? Passwords: ◦ must be only single-byte characters ◦ are case sensitive. When you log on you will have to enter your password exactly as you enter it here ◦ must be at least 8 characters long ◦ must not be longer than 31 characters ◦ cannot contain any spaces, and can contain only numbers (0-9), upper and lower case letters (A-Z, a-z), hyphens (-), underscore (_), periods (.), and the @ character

Figure A1.

About the authors

Kristen K. Greene is a Cognitive Scientist in the Visualization and Usability Group within the Information Technology Laboratory at the National Institute of Standards and Technology (NIST). She has an MA and a PhD in cognitive psychology from Rice University. She is an experienced research scientist, having conducted research in the Attention and Perception Laboratory at the University of South Carolina, the Usability Testing and Analysis Facility at NASA Johnson Space Center, the Computer Human Interaction Laboratory at Rice University; and now the Information Technology Laboratory at NIST. Kristen K. Greene is the corresponding author and can be contacted at: kristen.greene@nist.gov

Yee-Yin Choong is a Cognitive Scientist in the Visualization and Usability Group within the Information Technology Laboratory at the National Institute of Standards and Technology (NIST). Her research interests include user-centered design and evaluation methodology, usable security, public safety communications, biometrics usability and human factors. Prior to joining NIST, she practiced usability engineering in industry for 10 years. Her work included telecommunications, business-to-business eCommerce, Web applications and software internationalization. She received her MS degree in Industrial Engineering from the Pennsylvania State University and her PhD in Human Factors from Purdue University.