SCIENCE CHINA
Information Sciences

• **Supplementary File** •

On the User Friendliness of Password Creation Policy Designs in the Wild

Ding WANG[1,2,3], Tongxin WEI[1,2,3] & Zhenduo HOU[1,2,3*]

[1]*College of Cryptology and Cyber Science, Nankai University, Tianjin* 300350*, China; wangding@nankai.edu.cn;*
[2]*Key Laboratory of Data and Intelligent System Security (Nankai University), Ministry of Education, Tianjin* 300350*, China;*
[3]*Tianjin Key Laboratory of Network and Data Security Technology, Tianjin* 300350*, China*

Appendix A User study

Online Survey Instrument

In this survey, we invite you to step into the shoes of a character named Bob. Consider that this account holds significant value to you, similar to other key accounts you might possess, including those for email, banking, or social media platforms. Completing this survey is expected to take around 10 minutes.

The initial question. When you create a password on the web service, which of the following methods do you usually use? [Multiple choice]

☐ Design and create a password independently
☐ Use a password generated randomly by the system
☐ Use a password manager to generate a password
☐ Use a password similar or consistent with another account' password
☐ Automatically generate a password through social media or third-party accounts (not password manager)
☐ Other, please specify _____

Part One: Understanding of PCPDs User-friendliness

Generally, a Password Creation Policy Design (PCPD) is composed of a Password Rule (PR), a Password Registration Error Message (PREM), and a Password Strength Meter (PSM). we present and provide a detailed introduction to the various PCPD in different scenarios. Please estimate the level of user-friendliness in the following scenarios.

Password Rule (PR): Below are some introductions of PR in three different scenarios. Please refer to some examples (see Figs. F4, F5, F6 and F7) for more details.

Scenario PR1: When a user enters the registration page, the interface *directly presents* the password rules, like forbes.com.

Scenario PR2: The site does not timely display the password rules. When the user *enters a password* in the password input box, the site *will provide* password rules, like etsy.com.

Scenario PR3: A user enters a password and *clicks the Submit Button*; If the password fails *to meet* the password rules, the site will *show* the password rules, like wikihow.com.

Q1-3. Password Rule: Please rate the following evaluation criteria. (5 is the highest score). [Matrix scale questions]

Scenario PR1 (Directly display PR)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Set a unique password according to the web services' password rules
☐ Design a password similar to other account passwords according to the web services' password rules
☐ Design a simple password
☐ Design a longer password
☐ Design a password with more complex type characters
☐ Try and check error feedback before designing the password
☐ Use a password generated randomly by the system
☐ Give up registration
☐ Not sure
☐ Other (please specify)

Scenario PR2 (Receive password then display PR)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Set a unique password according to the web services' password rules
☐ Design a password similar to other account passwords according to the web services' password rules
☐ Design a simple password
☐ Design a longer password
☐ Design a password with more complex type characters
☐ Try and check error feedback before designing the password
☐ Use a password generated randomly by the system
☐ Give up registration
☐ Not sure
☐ Other (please specify)

Scenario PR3 (Click Submit Button then display PR)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know

* Corresponding author (email: joehou13@nankai.edu.cn)

Password behaviors: [Multiple choice]
☐ Set a unique password according to the web services' password rules
☐ Design a password similar to other account passwords according to the web services' password rules
☐ Design a simple password
☐ Design a longer password
☐ Design a password with more complex type characters
☐ Try and check error feedback before designing the password
☐ Use a password generated randomly by the system
☐ Give up registration
☐ Not sure
☐ Other (please specify)

Please explain how the display of password rules forms affects your password creation experience. [Free text]

Q4. What do you think are the reasons that lead you to use the same or similar passwords across multiple accounts? [Multiple choice]
☐ Simplified memory
☐ Unclear password creation rules on web services
☐ Saving effort in designing passwords
☐ No tool to store passwords
☐ Web services' password rules do not explicitly forbid using the same or similar passwords
☐ Too many accounts and passwords to manage
☐ Personal habits
☐ Other (please specify)

Password Error Message (PREM): Below are some introductions of PREM and the three scenarios. Please refer to some examples (see Figs. F8, F9, F10 and F11) for more details.

Scenario PREM1 (no feedback): When a user enters a password that does not meet the requirements of the password rules, the site will *refuse to register with no feedback* message.

Scenario PREM2: When a user enters a password that fail to satisfy the password rules, the site will send a wrong message, but the content of *PREM is nothing*, like okta.com.

Scenario PREM3: When a user enters a password that fail to satisfy the password rules, the site will *feedback on all specific password requirements* that are not met, like fastly.net.

Scenario PREM4: When a user enters a password that fail to satisfy the password rules, the site will *feedback a PREM step by step (i.e., one by one)*, like paypal.com.

Q5-8. Password Error Message (PREM): Please rate the following criteria. (5 is the highest score).[Matrix scale questions]
Scenario PREM1 (No feedback)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Uncertain about the reason, try continuously testing the password
☐ Refer to other accounts' passwords
☐ Refer to other web services' password rules
☐ Feel pressured and might give up modifying or changing the password
☐ Continue trying until find the correct password
☐ Use a password generated randomly by the system
☐ Give up registration
☐ Other, please specify: _____
Scenario PREM2 (No explanation)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Uncertain about the reason, try continuously testing the password
☐ Refer to other accounts' passwords
☐ Refer to other web services' password rules
☐ Feel pressured and might give up modifying or changing the password
☐ Continue trying until find the correct password
☐ Use a password generated randomly by the system
☐ Give up registration
☐ Other, please specify: _____
Scenario PREM3 (Fully display all PREM)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Check item by item and modify multiple times based on the error message until it meets the requirements
☐ Check thoroughly and successfully modify once with the error message
☐ Refer to other accounts' passwords
☐ Refer to other web services' password rules
☐ Feel pressured and might give up modifying or changing the password
☐ Continue trying until find the correct password
☐ Use a password generated randomly by the system
☐ Give up registration
☐ Other, please specify: _____
Scenario PREM4 (Step by step feedback PREM)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Check item by item and modify multiple times based on the error message until it meets the requirements
☐ Check thoroughly and successfully modify once with the error message
☐ Refer to other accounts' passwords
☐ Refer to other web services' password rules
☐ Feel pressured and might give up modifying or changing the password
☐ Continue trying until find the correct password
☐ Use a password generated randomly by the system
☐ Give up registration
☐ Other, please specify: _____

Please describe the impact of PREM on your password registration. [Free text]

Q9. When creating a password, due to the web services' password policy restrictions (e.g., insufficient password length, limited character types), the most frequent number of times you modify the password is:

○ 1 time; ○ 2 times; ○ 3 times; ○ 4 times; ○ 5 times; ○ More than 5 times; ○ Not sure

(*if 1<times is selected*) How does modifying the password impact you?

☐ Increase password forgetting, especially when passwords become more complex or frequently changed
☐ Increase security risks, choosing easily memorable passwords that are not strong enough or easy to guess
☐ Increase password reuse, such as using the same or similar passwords across multiple accounts
☐ Increase reliance on password managers, without appropriate management tools, it is easy to forget passwords
☐ Increase account recovery difficulty, if forgotten after changing a password, account recovery may become difficult
☐ No significant impact
☐ Other, please specify:

Password Strength Meter (PSM): Below are some introductions to PSM (see Figs. F12, F13, F14 and F15).

Scenario PSM1 (no PSM): The site does *not provide password strength meter*.

Scenario PSM2: The site only *provides feedback of "Strong" or "Weak"* for the strength of the password, like dell.com.

Scenario PSM3: The site *not only* provides feedback on the password strength *but also* gives textual suggestions to help improve the password, like etsy.com.

Scenario PSM4: The site *allows* popular passwords, like dell.com.

Scenario PSM5: The site *blocks* popular passwords, like zillow.com.

Q10-14. Password Strength Meter (PSM): Please rate the following evaluation criteria. (5 is the highest score) [Matrix scale questions]

Scenario PSM1 (No PSM)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Overlook password security
☐ Choose simple passwords
☐ Increase the complexity of my password to enhance its strength
☐ Difficulty in determining if my password is strong enough
☐ Make me rely on memory and experience when designing passwords
☐ Feel uncertain, may give up registration
☐ Use a password generated randomly by the system
☐ Refer to other accounts' passwords
☐ Refer to other web services' password strength feedback
☐ Other, please specify: _____

Scenario PSM2 ("Strong" or "Weak"Feedback)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Adjust my password based on password strength
☐ Increase the complexity of my password to enhance its strength
☐ Feel confused without specific suggestions
☐ Ignore password strength and choose simple passwords
☐ Feel uncertain, may give up registration
☐ Use a password generated randomly by the system
☐ Refer to other accounts' passwords
☐ Refer to other web services' password strength feedback
☐ Other, please specify: _____

Scenario PSM3 (Text explanation)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Adjust my password based on password strength
☐ Increase the complexity of my password to enhance its strength
☐ Feel confused without specific suggestions
☐ Ignore password strength and choose simple passwords
☐ Feel uncertain, may give up registration
☐ Use a password generated randomly by the system
☐ Refer to other accounts' passwords
☐ Refer to other web services' password strength feedback
☐ Other, please specify: _____

Scenario PSM4 (Allow popular passwords)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know

Scenario PSM5 (Block popular passwords)
User-friendliness with text presentation efficiency: ○1 ○2 ○3 ○4 ○5 ○ Don't know
User-friendliness with friendly-explanation: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Password behaviors: [Multiple choice]
☐ Design a unique and stronger password
☐ Refer to other accounts' passwords
☐ Try to modify a popular password to make it more secure
☐ Rely on a password manager to generate and store a new password
☐ Use a password generated randomly by the system
☐ Give up the registration
☐ Other, please explain: _____

Please describe the impact of PSM on your password. [Free text]

Q15. Do you need a password strength reminder in password registration? ◯ Yes ◯ No ◯ Don't know

Q16. Please select the scenario that is more friendly.

◯ Scenario PSM2 ("Strong" or "Weak" feedback) ◯ Scenario PSM3 (Text explanation) ◯ Don't know

Q17. Please select the scenario that is more friendly.

◯ Scenario PSM4 (Allow popular passwords) ◯ Scenario PSM5 (Block popular passwords) ◯ Don't know

Other components:

Q18-26. Please estimate the level of user-friendliness in the following scenarios. [Matrix scale questions]

OC1: The site provides a *system-assigned password*. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know

OC2: The site provides a *show* password button. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know

OC3: The site asks the user to confirm the password *again*. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know
OC4: The site requires users to design a *unique username*. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know
OC5: The site requires users to *human machine verification*. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know
OC6: The site allows users to *copy* passwords to other interfaces. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know
OC7: The site allows users to *paste* content from other interfaces into the password box. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know
OC8: The site requires users to complete and supplement the user's *personal information*. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know
OC9: The site requires users to enter a *captcha and human machine verification*. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Q27. Please sort the user-friendliness of the above nine components. (5 represents the most friendly) [Sort the items]
Please describe the impact of the above nine components on your password registration. [Free text]
Q28-29. Please estimate the level of user-friendliness in the following scenarios. [Matrix scale questions]
Rule 1: If a password meets the specific password rules, the site will allow registration. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Rule 2: Sites allow registration when user-designed passwords satisfy both the site's specific password rules and meet the required password strength. User-friendliness: ○1 ○2 ○3 ○4 ○5 ○ Don't know
Q30. Please choose the password requirement that is more user-friendly. ◯ Rule 1 ◯ Rule 2 ◯ Don't know
Q31. Please rank the user-friendliness of PCPDs based on the impact of critical components on user experience. [Sort the items]
○Password Rule (PR) ○Password Registration Error Message (PREM) ○Password Strength Meter (PSM) ○Other Components (OC)
[Free text] Please provide an explanation for the results of your sorting.
Part Two: Basic Information of Respondents
Q32. What is your gender? ○Female ○Male ○Non-binary ○Other_____ ○No response
Q33. How old are you? ○18-25 years old ○26-35 years old ○36-45 years old ○46-55 years old ○56-65 years old ○66 or older ○No response
Q34. What is your educational background?
○Below bachelor degree
○Bachelor's degree or equivalent
○Master's degree or equivalent
○Doctor degree or equivalent
○Prefer not to say
○Other (please specify)
Q35. What is the relevance of your professional background to the cybersecurity category (e.g., cryptographic science and technology, information security, cyberspace security, etc.)? ○Irrelevant ○Not relevant ○Normal ○Relevant ○Highly relevant ○No response
Q36. How familiar are you with password security?
○Not familiar ○Basic (I use password only) ○Familiar (I can perform normal tasks) ○Developer/Professional ○No response
Q37. How many password accounts do you have? ○1-5 ○6-10 ○11-15 ○16-20 ○20+ ○No response
Q38. (Optional) If you have any comments or suggestions, please leave a message here. [Free text]

Table A1 Design of other components in password registration on Chinese and English sites.*

Other components	Chinese sites (N = 163)	English sites (N = 202)
System-assigned password	127	93
Show password	103	129
Confirm password	87	66
Unique username	34	46
Help design username	13	18
Human machine verification	18	22
HMV and captcha	101	56
Paste password	157	201
Copy password	45	109
Mobile phone number	125	39
Bind phone number	116	35
Email address	24	185
Bind Email	13	78
Personal information	31	133
Rules1	146	136
Rules2	17	66

*HMV = Human machine verification. Rules 1 means specific length or characters of password requirements. Rules 2 means requirements beyond Rule 1, e.g., password blacklist.

Appendix B Offline interview

We classify the websites into four groups to understand the effect of different elements on the account registration process. Each group is designed to focus on a unique condition, setting it apart from the others. This approach allows us to isolate and analyze the impact of individual components on user registration experiences. (see Table B1). At the end of the interview, we inform participants not to use the password samples we provide in future activities, even though some of these passwords are rated as strong by various web services.
1. How do you describe your experience creating a secure password using the those password creation policy designs? Is it easy or challenging, and why?
2. Which of the three (four) password creation policy designs in the experiment do you feel is the most effective or user-friendly? Why?
3. Which of the following Password Creation Policy Designs do you prefer? Please rank them in order of preference and explain your reasons.
(a) We provide a link to the web service (refer to the Table B1). Please click on the account registration option directly on the site and complete the password creation process there.

(b) Click on the account registration link on the site, and you will be redirected to the web service through the browser on your laptop.

(c) Users are required to go through the entire account registration process.

4. Among those password creation policy designs, which one do you feel is the most user-friendly or effective? Why?

5. Did you face any difficulties (e.g., understanding password rules, navigating the site, or responding to error messages) while performing the task?

(Questions 6 to 8 were asked only if the participant indicated experiencing difficulties during registration.)

6. Do you believe the account creation process could be improved? If so, how?

7. Did you notice any error messages displayed during password registration? If so, what stood out to you, and why?

8. What do you think about the display forms of the password rules? Are they easy to follow?

9. What is your opinion of the password strength meter? Do you think its results were helpful or accurate? Please explain why or why not.

Table B1 Sites password creation policy designs during registration.*

		PR			**PREM**				**PSM**					**SR**		**Other Components**								
	Sites	1: Directly Display	2: Enter then Display	3: Click Submit Button then Display	1: Nothing Feedback	2: No Explanation but Warning	3: Fully Feedback	4: Step-by-step Feedback	1: No PSM	2: Color Bar	3: Text Explanation	4: Allow the popular Passwords	5: Block the popular Passwords	1: Specific Password Rules	2: Rule1 + Other Requirements	1: System-assigned Password	2: Show Password	3: Confirm Password	4: Unique Username	5: Help Design Username	6: Man-machine Verification	7: Paste Password	8: Copy Password	9: Add Personal Information
PR	*forbes.com*	⊕	⊖	⊖			⊙			⊙				⊙			⊙	⊙				⊙	⊙	⊙
	amazonaws.com	⊖	⊕	⊖			⊙		⊙						⊙		⊙	⊙				⊙		⊙
	microsoft.com	⊖	⊖	⊕				⊙	⊙						⊙		⊙	⊙			⊙	⊙		
	chaoxing.com	⊕	⊖	⊖			⊙		⊙					⊙		⊙	⊙					⊙	⊙	
	www.adobe.com	⊖	⊕	⊖			⊙		⊙					⊙		⊙	⊙					⊙	⊙	
	3dmgame.com	⊖	⊖	⊕			⊙		⊙					⊙		⊙		⊙				⊙		
PREM	*forbes.com*	⊙			⊖	⊖	⊕	⊖		⊙				⊙			⊙	⊙				⊙	⊙	⊙
	twitter.com	⊙			⊖	⊖	⊖	⊕	⊙					⊙		⊙						⊙		
	gandi.net	⊙			⊖	⊕	⊖	⊖			⊙				⊙		⊙					⊙	⊙	⊙
	sciencedirect.com	⊙			⊕	⊖	⊖	⊖		⊙					⊙	⊙						⊙		⊙
	kuaidi100.com	⊙			⊕	⊖	⊖	⊖	⊙					⊙		⊙						⊙		
	job592.com	⊙			⊖	⊖	⊕	⊖	⊙					⊙		⊙						⊙		
	360.cn	⊙			⊖	⊖	⊖	⊕	⊙					⊙		⊙						⊙		
	leleketang.com	⊙			⊖	⊕	⊖	⊖	⊙					⊙		⊙						⊙		
PSM	*google.com*			⊙				⊙	⊕	⊖	⊖	⊖	⊖	⊙			⊙	⊙				⊙	⊙	⊙
	apple.com		⊙				⊙		⊖	⊕	⊖	⊕	⊖		⊙			⊙				⊙	⊙	⊙
	www.12306.cn	⊙						⊙	⊖	⊕	⊖	⊖	⊕	⊙		⊙		⊙				⊙		⊙
	job592.com	⊙					⊙		⊕	⊖	⊖	⊖	⊖	⊙		⊙						⊙		
	51credit.com	⊙					⊙		⊖	⊕	⊖	⊕	⊖	⊙		⊙						⊙		
	weibo.com	⊙					⊙		⊖	⊖	⊕	⊕	⊖	⊙		⊙						⊙		
SR	*cq.gov.cn*	⊙					⊙		⊙					⊖	⊕	⊙		⊙	⊙		⊙	⊙		⊙
OC[5)]	*job592.com*	⊙					⊙		⊙					⊙		⊕						⊙		
	microsoft.com	⊙					⊙		⊙					⊙		⊖						⊙		
	chaoxing.com	⊙					⊙		⊙					⊙		⊙	⊕					⊙	⊙	
	job592.com	⊙					⊙		⊙					⊙		⊙	⊖					⊙		
	aliyun.com	⊙					⊙		⊙					⊙		⊙	⊙	⊕				⊙	⊙	
	chaoxing.com	⊙					⊙		⊙					⊙		⊙	⊙	⊖				⊙	⊙	
	s.1688.com	⊙					⊙		⊙					⊙		⊙		⊙	⊕			⊙		
	focus.cn	⊙					⊙		⊙					⊙		⊙		⊙	⊖			⊙		
	fang.com	⊙						⊙	⊙					⊙		⊙	⊙			⊕		⊙	⊙	
	s.1688.com	⊙					⊙		⊙					⊙		⊙		⊙	⊙	⊖		⊙		
	qianzhan.com	⊙					⊙		⊙					⊙		⊙					⊕	⊙		
	job592.com	⊙					⊙		⊙					⊙		⊙					⊖	⊙		
	job592.com	⊙					⊙		⊙					⊙		⊙						⊕	⊖	
	gamersky.com	⊙					⊙		⊙					⊙		⊙						⊖	⊖	
	chinaxinge.com	⊙					⊙		⊙					⊙		⊙		⊙	⊙			⊙		⊕
	s.1688.com	⊙					⊙		⊙					⊙		⊙		⊙	⊙			⊙		⊖

*PR = Password Rule; PREM = Password Registration Error Message; PSM = Password Strength Meter; SR = successful Registration; OC = Other Components. Numbers (1, 2, 3...) represent different components, which are corresponding to the horizontal title. ⊖ represents control group, and ⊕ represents evaluation conditions; ⊙ represents sites' PCPDs.

Appendix C Codebook

We supply a comprehensive codebook, which encompasses primary codes, their corresponding counts, and initial-level sub-codes.

∘**Account numbers (96):** <5 (30), 5-10 (26), 11-15 (19), 16-20 (5), 20+ (16).

∘**Familiarity with password registration (35):** basic (20), familiar (10), developer/professional (5).

∘**Attitude towards password registration (21):** Impatient with the registration process (6), the registration process is simple and user-friendly (3), frustrated with having to register repeatedly for each account(12).

∘**Reasons for the attitude (15):** Passwords are easy to remember (5). Quick authentication in daily (7). Current site security mechanisms are robust and effective (3).

∘**Difficulty level of password registration (25):** difficult(3), easy (18), very easy (4).

∘**Factors hindering password registration (41):** strict password requirements (23), frequent password changes (7), lack of education (2), security concerns (6), inconvenient registration process (3).

∘**Demand for password registration (58):** not needed at all (2), not needed (3), neutral (18), needed (23), highly needed (12).

∘**Usability of password rule (53):** clear and concise display of rules (28), examples or sample passwords (5), optional rule explanations/help features (6), customizable rule settings (11).

∘**Security of password rule (51):** Strong password requirements (18), no leakage of sensitive information (5), prevention of brute force attacks (3), protection of password information in transmission and storage (7), provision of additional authentication factors (16), timely updating of password rules (2).

∘**The reasons that can influence users' preference for PR (87):** ease of understanding (45), usability (13), consistency (7), trust and credibility (10), relevance and personal connection (12).

∘**Usability of password registration error message (47):** password length requirements (22), complexity requirements (4), uniqueness (2), low password security (3), password confirmation mismatch (16).

∘**Security of password registration error message (37):** enhance password security, prevent weak password usage (28), restrict password history (4), remind password expiration (2), detect abnormal login behavior (3).

∘**Acceptable password registration error message (15):** ease of understanding (8), visual presentation (3), personalization (1), and consistency (3).

∘**The reasons influencing users' preference for PREM (24):** clarity (5), detailed explanations (2), specific guidance (5), visual presentation (5), timely feedback (7).

∘**Needs for the password strength meter (55):** not needed at all (2), not needed (6), neutral (8), needed (18), highly needed (21).

∘**Usability of password strength meter (29):** providing guidance (21), facilitating quick assessments (1), and enhancing security (7).

∘**Security of password strength meter (25):** increasing password security (18), refusing weak passwords (4), promoting password complexity (2), enhancing overall system security (1).

∘**Acceptable password strength meter (19):** popular types include length and character type-based strength meters (11), dictionary matching checks (2), rule-based evaluations (5), and visual strength indicators (1).

∘**The reasons influencing users' preference for PSM (42):** accuracy (18), conflict (2), consistency (3), reliability (5), explanations (5), personalization (1), specific suggestions (7), efficiency (1).

∘**The factors that can influence users' preference for OC(188):** system-assigned passwords(28), show button(21), confirm password(11), unique username(3), human-machine verification(14), copy operation(9), paste operation(17), fill personal information(22), enter a captcha(5), vulnerability to attacks(16), registration efficiency(18), operation steps(21), and time required(3).

∘**Security awareness in password creation (51):** use common passwords (22), personal information-based passwords (13), or longer passwords (16).

∘**Differentiated treatment (19):** security concerns (6), convenience (13).

∘**Password security risk warning (43):** clear (6), real-time (12), guidance and recommendations (8), multi-factor authentication recommendation (4), regular reminders and updates (13).

∘**User-friendliness with current site password registration (42):** satisfied (7), dissatisfied (16), neutral (19).

∘**Expectations for the password registration process (57):** Simplicity and clarity (8), security measures (6), user-friendly interface (7), Quick completion (12), information protection (9), Multiple registration methods (13), reliable account verification (2).

∘**Miscellaneous themes:** CR1: Complexity requirements too strict. CR2: Complexity requirements not clear. CR3: Flexibility needed in complexity requirements. SM1: Appreciate two-factor authentication. SM2: Password strength check needs improvement. SM3: Account lockout helpful. UI1: User-friendly interface. UI2: Clear instructions and prompts. UI3: Visual indicators of password strength. PM1: Difficulty managing multiple passwords. PM2: Suggest password manager. PM3: User-friendly password reset. PS1: Need secure password sharing. PS2: Suggest encrypted password sharing. PS3: Clear guidelines on safe password sharing. UX1: Quick and convenient process. UX2: Seamless integration with other platforms. UX3: Suggest autofill or password suggestion. PS1: Concerns about privacy and security. PS2: Clear communication of privacy policies. PS3: Recommendations for password safeguarding.

Table C1 Users' perceptions of friendly password creation policy designs ranks.*

	American participants (N = 139)					**Chinese participants (N = 96)**				
	Score	Rank 1	Rank 2	Rank 3	Rank 4	Score	Rank 1	Rank 2	Rank 3	Rank 4
Password Rule (PR)	**3.48**	**86(61.87%)**	24(17.27%)	26(18.71%)	3(2.16%)	**3.36**	**52(54.17%)**	32(33.33%)	7(7.29%)	5(5.21%)
Password Registration Error Message	**2.85**	26(18.71%)	**57(41.01%)**	45(32.37%)	11(7.91%)	**2.56**	15(15.63%)	33(34.38%)	**39(40.63%)**	9(9.38%)
Password Strength Meter (PSM)	**2.46**	26(18.71%)	**53(38.13%)**	43(30.94%)	17(12.23%)	**2.82**	28(29.17%)	28(29.17%)	**35(36.46%)**	5(5.21%)
Other Components	**1.19**	1(0.72%)	5(3.6%)	25(17.99%)	**108(77.7%)**	**1.25**	1(1.04%)	3(3.13%)	15(15.63%)	**77(80.21%)**

*The Score and Rank represent the degree of impact on the overall sign-up user-friendliness.

Appendix D User study results

In our online study, Chinese and American participants have consistent perceptions of user-friendliness in PR, PREM, and PSM (see Fig. D1). Users have varying opinions on how different components affect their password creation process. According to the importance ranking provided by the users, the U.S. participants are ranked as follows: PR (score: 3.48), PREM (score: 2.85), PSM (score: 2.46), OC (score: 1.19). For the participants from China, the ranking differs for PREM and PSM, and the ranking is as follows: PR (score: 3.36), PSM (score: 2.82), PREM (score: 2.56), OC (score: 1.25). We also provide the impact of those components on user-friendliness in password registration (in Supplement file). In the interviews, participants express various opinions and frustrations regarding interface designs. *"I hate registering personal information because it wastes time and threatens my privacy."* (P17) *"Some human-machine validations are too difficult to understand, which hinders me from registering."* (P12) *"Email and phone numbers are unique, why create a unique user name to add to the burden of memory?"* (P14) *"When I register, the verification code is not received in my email, causing registration to fail."* (P8)

To analyze the reasons behind the differences between Chinese and American participants, we inversely evaluate the users' account numbers about the user-friendliness scores (Q5, Q6, Q35, Q37). 61% participants who speak Chinese tend to think the "Click submit button" display PRs is friendly. In PREM, 42% of Chinese participants think "Nothing feedback" is friendly (df=1, p-value<0.001) and 49% of Chinese participants think "No explanation" is friendly (df=1, p-value<0.001). Note that, in Q8, the proportion of participants who directly enter their passwords timely could be underestimated in practice because participants may believe this is the expectation of the researchers. To further learn users' awareness of PREMs in their registration practices, in our interview, most participants cannot come across the PREMs. However, in PSM, 29.8% (20/67) of Chinese participants consider having PSM as user-friendly, while 19.8% (21/106) of American participants consider it as friendly (df=1, p-value<0.001). Additionally, 64.5% (49/76) of Chinese users find it acceptable for sites to block weak passwords, while 54.9% (67/122) of American users hold opposing views (df=1, p-value<0.01), which hinders their registration. There are no significant differences in the display forms evaluation of user-friendliness between Chinese and American participants.

PCPD impacts users' efficiency in password creation and login. In our interview, password creation and login behaviors vary across different PCPDs, reflecting the impact of guidance and restrictions on user effort. If a user does not encounter PREM during password creation, they are not included in the count. "Block popular passwords" and "Step-by-step feedback" cost the longest creation times, 35 seconds and 32 seconds, due to repeated password rejections or interactive guidance. "No PSM" demonstrates the shortest times, with medians between 10–15 seconds. Highly interactive setups, "Step-by-step feedback" and "block popular passwords," have the highest median click counts, around 6–7, with ranges extending up to 12 clicks. "Directly display" and "Text explanation," result in the lowest click counts, with medians close to 1 or 2. However, due to the different password rules of the web service, the strength and choice of the password used by users have a great impact on these results, which is only a relative result rather than an absolute one.

There is no apparent correlation between participants' gender, major and their assessment of the user-friendliness of PCPDs. Our findings indicate that judgments of user-friendliness are not significantly influenced by participants' professional backgrounds, gender or native language. For instance, among Chinese participants, both male (88%, 51/58) and female (74%, 28/38) participants view PSM as friendly (Q15). Additionally, a significant majority of males (83%, 48/58) and most females (89%, 34/38) show a preference for popular passwords (Q17). Our research establishes a significant correlation between the educational backgrounds of Chinese participants and their views on the user-friendliness of PREM. Participants with lower educational levels are generally more receptive to certain PCPD practices. This preference for "No Explanation PREM" diminishes with increasing educational level: 41% (17/41) of undergraduate degree holders, 24% (6/25) of master's degree holders, and 11% (1/9) of doctoral degree holders think the PREM is friendly. Participants' responses in Q8 exhibit similar distribution patterns in their evaluation results.

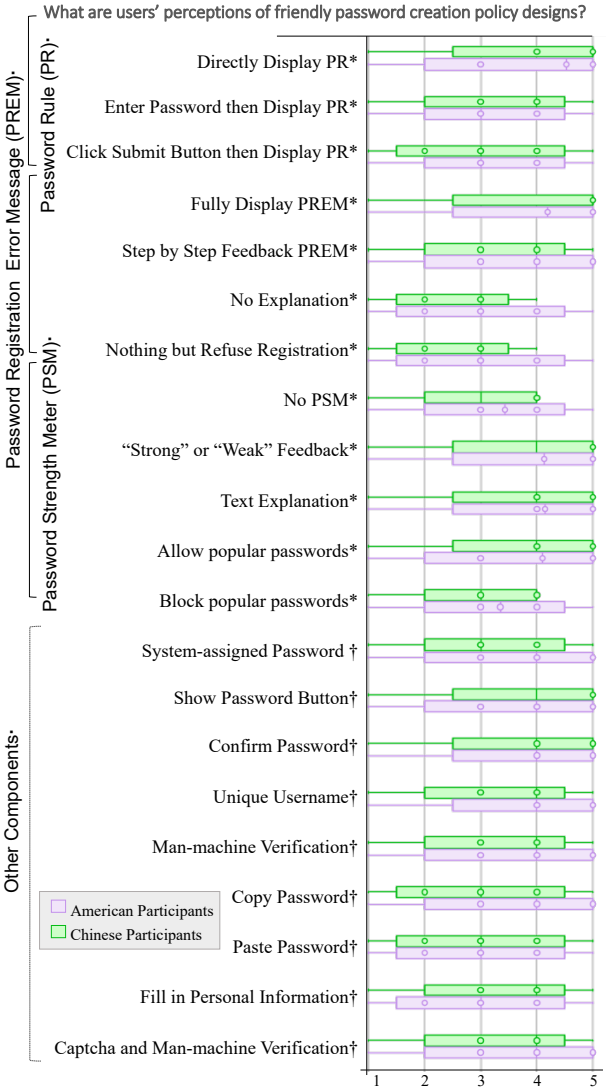


Figure D1 The user-friendly evaluation of Password Creation Policy Designs (PCPDs) in registration. The horizontal axis represents the percentage of different levels of user-friendliness towards the PCPDs, while the vertical axis corresponds to the relevant PCPDs. * represents what we define in PCPDs. † represents the other components in the process of password registration. The results show that Chinese and American participants have similar preferences for PCPDs.

Figure D2 The results of the time spent on user registration, the number of mouse clicks, and the number of error attempts during re-login.

Appendix E Web service survey

In this section, we present various password registration interfaces (see Figs. F4-F15). They conduct registrations following the sites' guidelines, with the inspection process outlined as follows:

1. Navigate to the user registration interface of the sites.
2. Examine the steps required for site registration.
3. Input the password samples and note interfaces' changes.
4. Record the design of these site interfaces.
5. Click the submit button to finalize the registration.
6. Record the registration processes and the designs of the password creation interfaces encountered in registration.

Other components. Table E2 shows the other components applied in Chinese and U.S. sites. Chinese sites tend to enforce stricter password policies and support multiple identity authentication methods (see Table E1). Additionally, 127/163 Chinese sites provide system-assigned passwords. 93/202 U.S. sites have looser password policies and offer fewer options for system-assigned passwords. Additionally, sites use human-machine verification during user identity binding (Chinese sites: 101/163; U.S. sites: 56/202), which can enhance account security by preventing automated bots from accessing user accounts. U.S. sites seem to be less likely to prevent users from pasting passwords (Chinese sites: 157/163; U.S. sites: 201/202) and copying passwords (Chinese sites: 45/163; U.S. sites: 109/202), which could potentially pose a risk of password leakage. 78/202 U.S. web services prefer users to link their emails, while 116/163 Chinese web services favor the binding of phone numbers. 133/202 U.S. websites commonly request personal information (PI) in the registration, a practice less prevalent among Chinese sites, with only 31/163 requesting PI. We find that most participants ignore or pay no attention to these components in registration. Besides, they desire to avoid spending additional time on registration operations. In password registration, over 80% of participants express that the show button (Q19) and the confirm password (Q20) are friendly. Many participants consider actions like (45%, 112/249) copying (Q23), (51%, 128/249) pasting (Q24) passwords as friendly, even though there is a risk of password leakage. Besides, 34.93% (87/249) of participants dislike the system-assigned passwords.

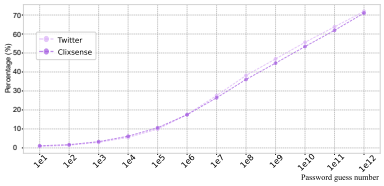
Table E1 Registration methods on Chinese and U.S. sites.

Sites rank	Available access	Password registration	No password registration	Email registration	Mobile phone registration	Three-party registration	No authentication	Unable to access
	Chinese sites							
1-100	98	**47**	29	-	28	22	22	2
101-200	93	**38**	27	-	25	18	28	7
201-300	86	**23**	22	-	19	10	41	14
301-400	86	**28**	26	-	21	22	32	14
401-500	84	**27**	29	2	19	16	28	16
Total	447	**163**	133	2	112	88	151	53
	U.S. sites							
1-100	63	**51**	6	2	5	4	6	37
101-200	50	**30**	10	2	5	6	10	50
201-300	68	**43**	7	3	2	7	18	32
301-400	67	**41**	16	7	3	10	10	33
401-500	71	**37**	17	6	5	10	17	29
Total	319	**202**	56	20	20	37	61	131

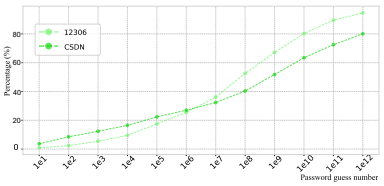
Table E2 Design of other components in password registration on Chinese and U.S. sites.*

Other components	**Chinese sites** (N = 163)	**U.S. sites** (N = 202)
System-assigned password	127	93
Show password	103	129
Confirm password	87	66
Unique username	34	46
Help design username	13	18
Human machine verification	18	22
HMV and captcha	101	56
Paste password	157	201
Copy password	45	109
Mobile phone number	125	39
Bind phone number	116	35
Email address	24	185
Bind Email	13	78
Personal information	31	133
Rules1	146	136
Rules2	17	66

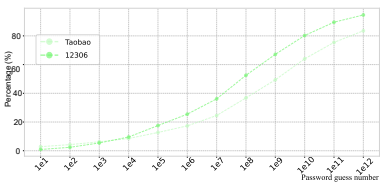
*HMV = Human machine verification. Rules 1 means specific length or characters of password requirements. Rules 2 means requirements beyond Rule 1, e.g., password blacklist.



(a) The impact of PR on password security.



(b) The impact of PREM on password security.



(c) The impact of PSM on password security.

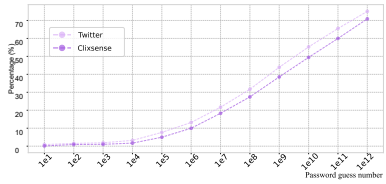
Figure F1 The percentage of passwords guessed is calculated by Random Forest with different password creation policy designs (training dataset: Dodonew).

Appendix F Chinese vs. English password security

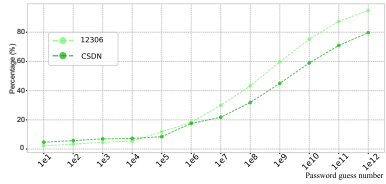
The English password is longer than the Chinese password. We validate Wang et al.'s claim that users' password lengths are distributed between 6 and 10 characters. We use Spearman correlation coefficients and multiple regression analysis to assess the impact of the user-friendliness of PCPD on users' password length and password entropy. We use zxcvbn to test the number of password guesses in the password dataset. Additionally, we find that users' password lengths follow a normal distribution. The Shapiro-Wilk test statistics for the datasets have an average value of 0.86, ranging from 0.81 to 0.97, and the p-values average 0.29, ranging from 0.09 to 0.87. Password lengths tend to be longer when websites deploy password blacklists (e.g., Wishbone, Yahoo, and CSDN). We observe a positive correlation between password length and password entropy in both Chinese and English datasets. The Spearman correlation coefficients are: Minimum (NA, not correlated), Q1 (0.797), Median (0.603), Q3 (0.718), and Maximum (0.92).

The English password entropy is higher than the Chinese password entropy. We calculate the password entropy. Passwords with repeated identical characters (e.g., "aaaaaa" or "111111") result in an entropy of 0, making it the minimum entropy value in the dataset.

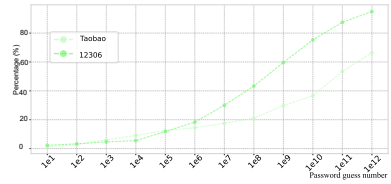
There is no significant correlation between the user-friendliness of PCPD and password length and entropy. PSM (length: r=0.329, p=0.323; entropy: r=0.273, p=417) shows a slightly stronger positive correlation with metrics compared to PR (length: r=0.276, p=0.412; entropy: r=0.315, p=0.345) and PREM (length: r=-0.092, p=0.788; entropy: r=-0.014, p=0.967), the results are not statistically significant. The multiple regression analysis reveals that PR, PREM, and PSM collectively explain a small proportion of the variance in password length (R^2 = 0.210) and password entropy (R^2 = 0.232). However, none of the factors demonstrate statistically significant effects on either password length or entropy, indicating limited influence.



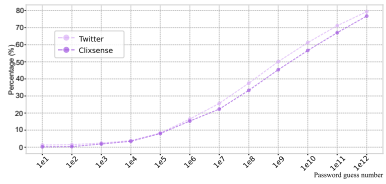
(a) The impact of PR on password security.



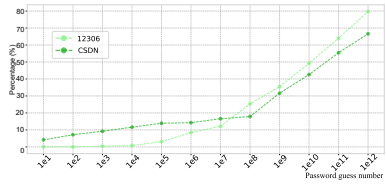
(b) The impact of PREM on password security.



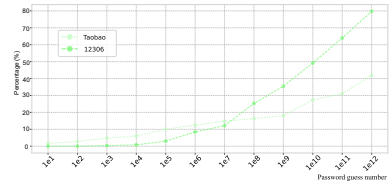
(c) The impact of PSM on password security.



(d) The impact of PR on password security.



(e) The impact of PREM on password security.

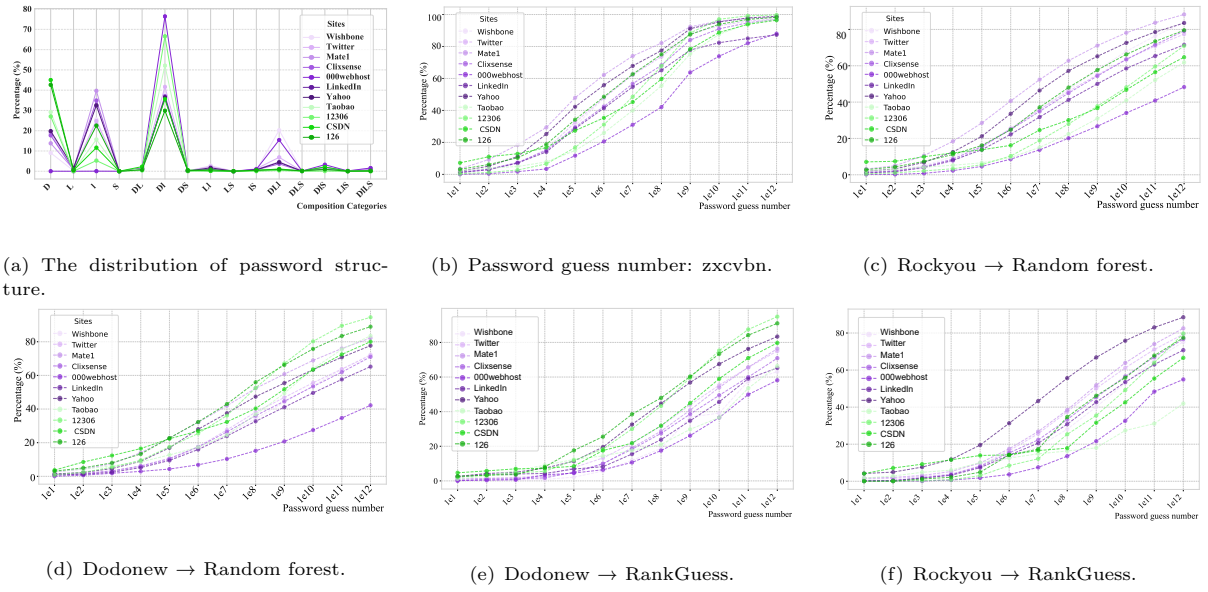


(f) The impact of PSM on password security.

Figure F2 The percentage of passwords guessed is calculated by RankGuess with different password creation policy designs. The training dataset for the first row is dodonew, and the training dataset for the second row is rockyou.

The composition of Chinese passwords is relatively simple, while English passwords exhibit greater diversity in character composition. Chinese users' passwords rely on numbers and letters, with a very low proportion of special characters (see Fig. F3). The passwords for 12306 have 81.2% numbers, and Taobao has 75.8% numbers, with a very small proportion of special characters. In contrast, English passwords, such as those for Twitter and LinkedIn, contain a wider variety of characters, with special characters accounting for 9.9% and 8.1%, respectively. The English datasets' passwords are more diverse in character types, with a relatively balanced proportion of uppercase letters, lowercase letters, numbers, and special characters, which helps improve the complexity and security of the passwords. For instance, Twitter's passwords consist of 55.8% letters (both uppercase and lowercase), 34.3% numbers, and 9.9% special characters.

The number of password guesses for Chinese passwords is higher than that for English passwords. While exhibit a peak in the 10^6 to 10^9 range, Chinese passwords demonstrate a higher proportion in stronger categories (10^9 to



(a) The distribution of password structure.

(b) Password guess number: zxcvbn.

(c) Rockyou → Random forest.

(d) Dodonew → Random forest.

(e) Dodonew → RankGuess.

(f) Rockyou → RankGuess.

Figure F3 The results of password character types, guessing numbers (calculated by zxcvbn), and perceptage of passwords guessed (calculated by RankGuess and Random forest). LlDS represents character types, including uppercase letters (L), lowercase letters (l), digits (D), and symbols (S). The training dataset for (c) and (f) is rockyou, while the training dataset for (d) and (e) is dodonew.

10^{12}), suggesting greater resistance to guessing attacks (see Fig. F3). English passwords are more concentrated in mid-strength categories. Notable differences emerge across websites: sites like CSDN and 12306 are skewed toward stronger Chinese passwords, whereas LinkedIn and Yahoo display weaker distributions for English passwords. We utilize zxcvbn to test the password guessing metrics in both English and Chinese password datasets. Taobao and 12306 exhibit high password complexity, particularly in the ranges of 10^7-10^8 and 10^8-10^9, accounting for 19.99% and 20.73%. Wishbone and Yahoo show notable distributions in the 10^4-10^5 and 10^5-10^6 ranges, at 15.84% and 16.89%.

The cracking success rate of Chinese password sets is higher when trained on Chinese datasets, while the cracking success rate of English password sets is higher when trained on English datasets. Mate1 and Clixsense display a more uniform password distribution, concentrated in the 10^3-10^5 range, suggesting a moderate level of password strength among users on these platforms. Notably, Mate1 exhibits a high percentage of 18.56% in the 10^4-10^5 range, suggesting a somewhat average level of password security. CSDN and 126 demonstrate lower complexity, with passwords primarily concentrated in the 10^5-10^6 range, accounting for 10.64% and 15.43%. 000webhost and LinkedIn show low levels of password complexity, particularly in the 10^2-10^3 range. The cracking rates of English password datasets (e.g., Wishbone, Twitter, Mate1) are generally higher, likely due to the prevalence of common words, phrases, and simple combinations (see Fig. F3). In contrast, Chinese password datasets (e.g., Taobao, 12306) exhibit lower cracking rates, likely attributable to the increased complexity introduced by Chinese characters and special symbols. For English password datasets, cracking rates increase progressively with password length, with a particularly sharp rise in the range above 10^6. While Chinese passwords also follow a similar upward trend, the rate of increase is notably more gradual, reflecting the added complexity of the passwords (see Fig. F3).

We use RankGuess to validate the above conclusion (see Fig. F2). We evaluate the password guessing resistance under different training datasets using Random Forest (see Fig. F1) and PCPD conditions with RankGuess on the Rockyou and Dodonew training datasets (see Fig. F2). In our RankGuess password resistance-to-guessing test, when the training set is Dodonew, before reaching 10^{18} guesses, Clixsense (95.6%) consistently outperforms Twitter (95.8%) in password resistance. However, when the number of guesses reaches 10^{19} to 10^{25}, the resistance difference between Clixsense (97.7%-99.5%) and Twitter (97.3%-98.7%) is less than 0.5%. Notably, Twitter's PR user-friendliness is higher than Clixsense's. For the 12306 dataset, before reaching 10^3 guesses, 12306 (4.6%) consistently outperforms CSDN (6.9%) in password resistance. However, once the number of guesses reaches 10^3, 12306's (10^{12}: 94.9%) resistance becomes lower than that of CSDN (10^{12}: 79.7%). CSDN's PREM user-friendliness is higher than 12306's. Taobao's (10^{12}: 66.3%) resistance-to-guessing performance remains consistently higher than 12306's (10^{12}: 94.9%), but Taobao does not have a PSM.

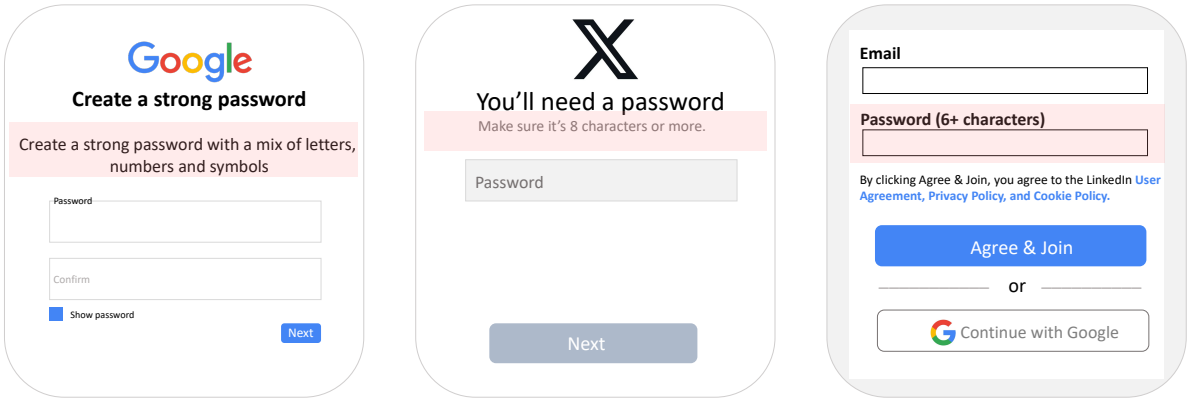


Figure F4 Display password rule directly: The website's password rules are shown immediately on the registration page before any user interaction (e.g., Google, Twiter, and LinkedIn).

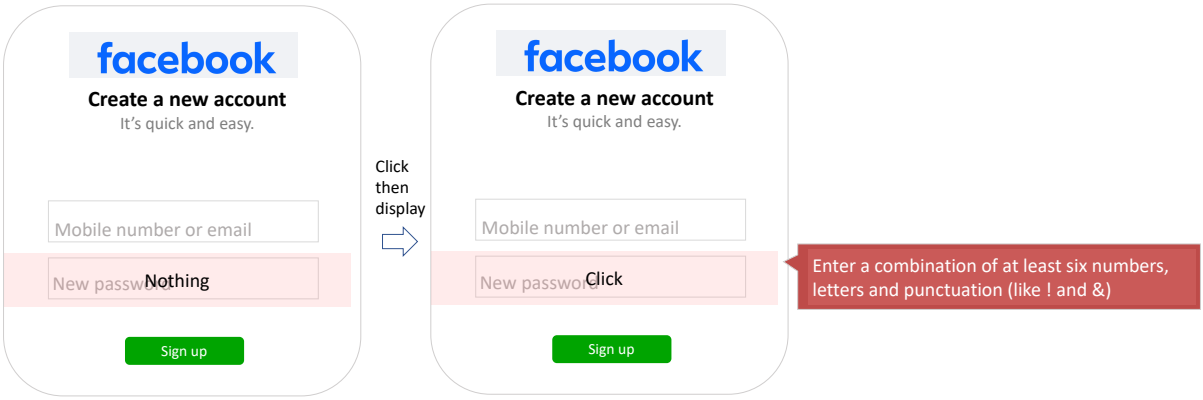


Figure F5 Display password rules after clicking the input field: Initially, the registration page shows no password rules. Once the user clicks on the password creation field, the website then displays the password rules.

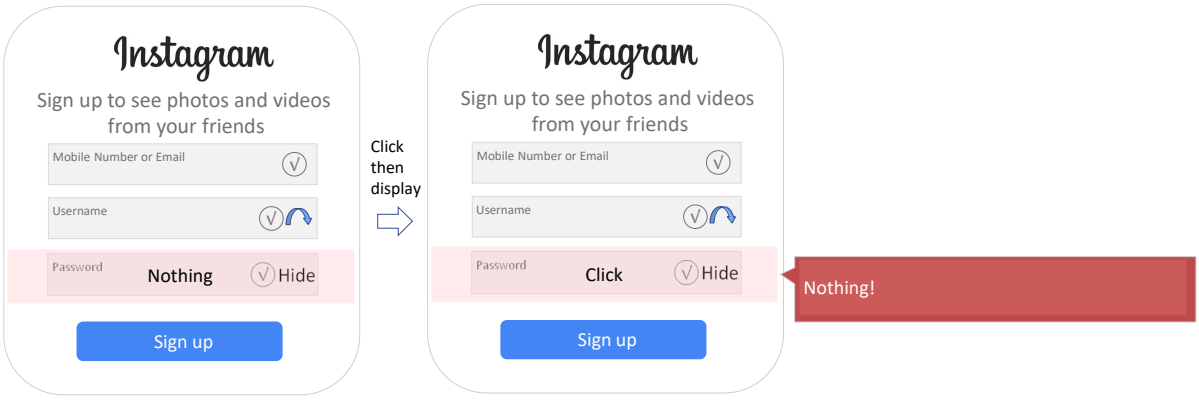


Figure F6 No password rules: The website does not display password rules, neither when clicking on the password input field nor while entering a password. Error messages appear when the submit button is clicked, but still no password rules are shown.

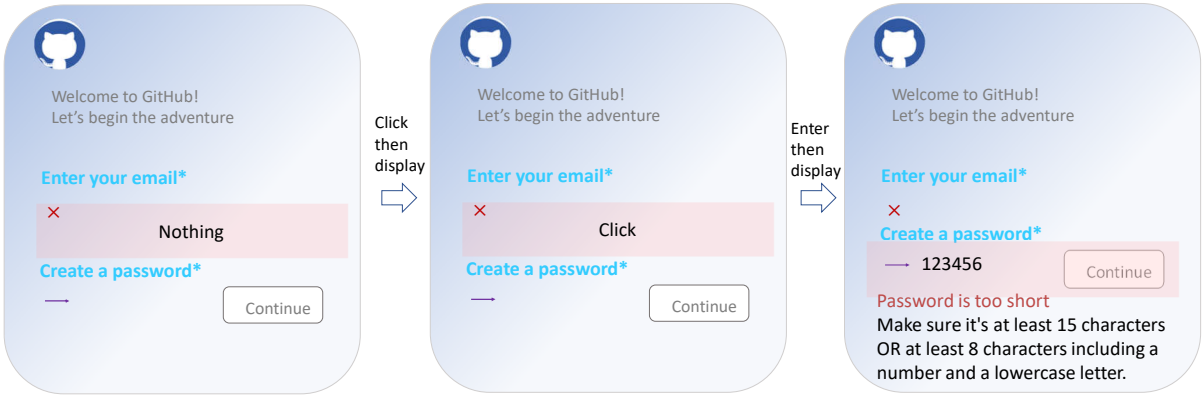


Figure F7 Display password rules after entering the password: On the registration page, clicking the password creation field does not display the password rules. The website only provides feedback on the password rules and error messages once the user begins entering a password into the field.

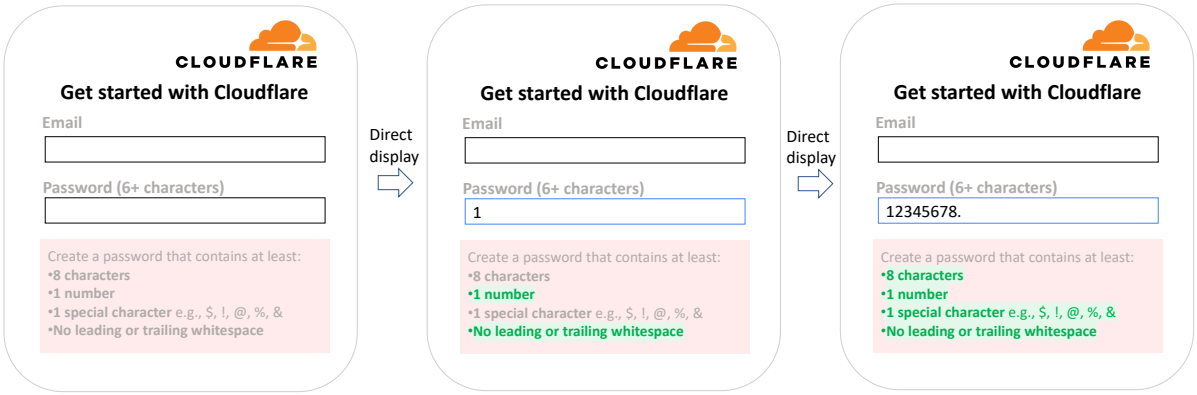


Figure F8 Display all password registration error messages: The website comprehensively lists all password creation requirements and provides real-time feedback on whether the user's password meets or fails each specific condition as they type.

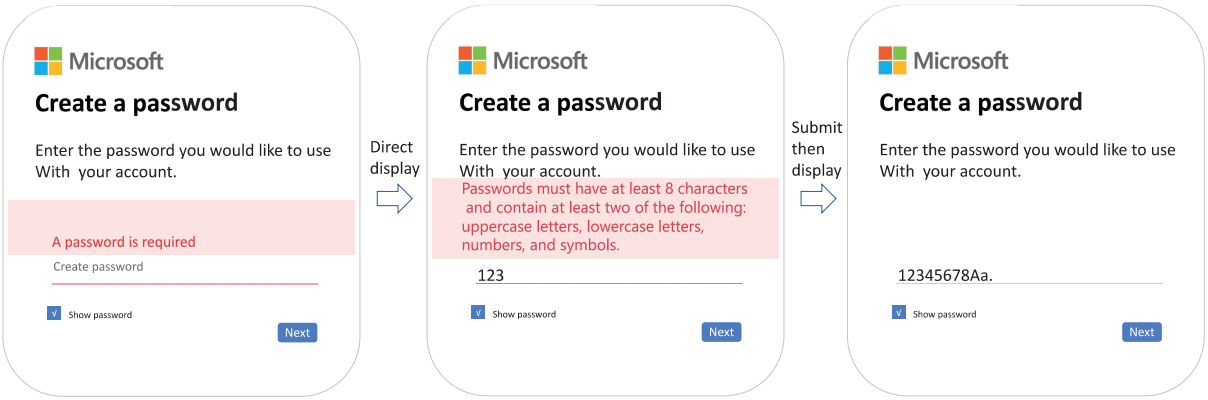


Figure F9 Display all password registration error messages at once: The website provides all the password rules, allowing users to create and modify their passwords by referencing these conditions themselves.

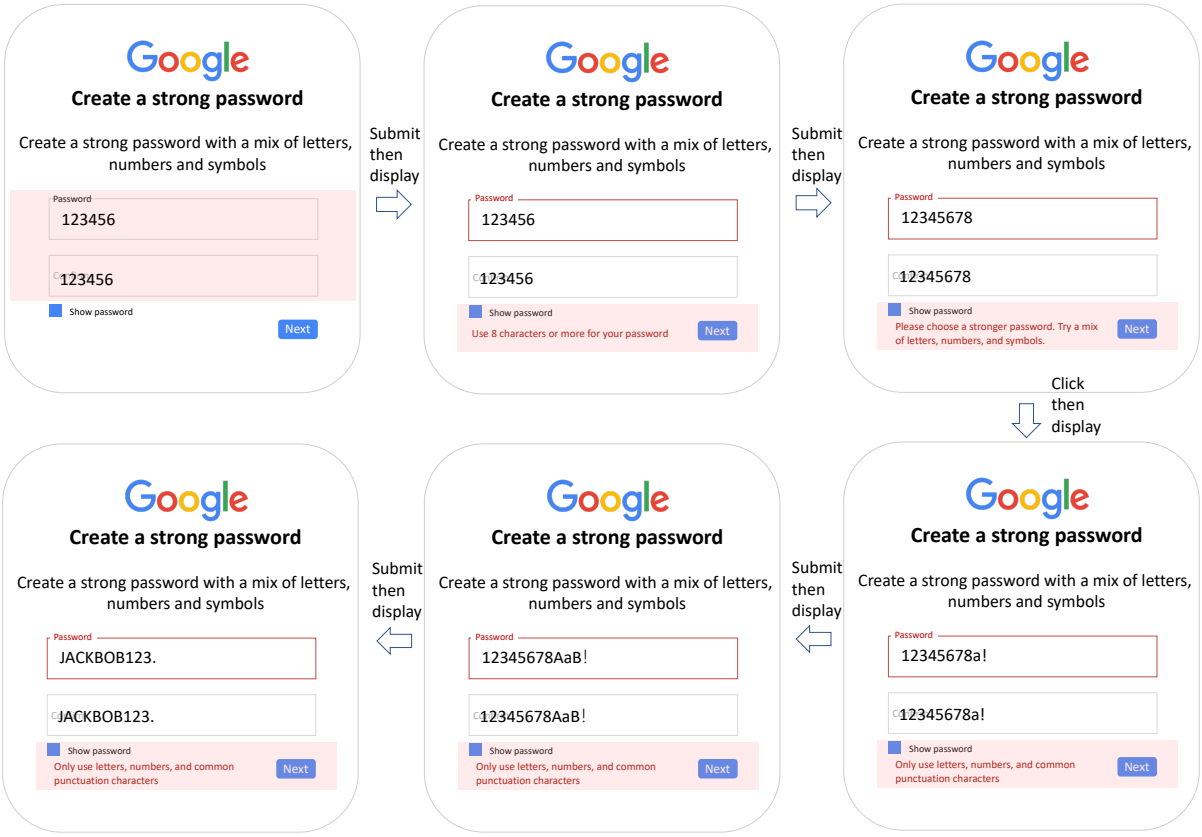


Figure F10 Display password registration error messages step-by-step: The website provides feedback based on the user's input, indicating which password requirements are not met by the current password, one by one.

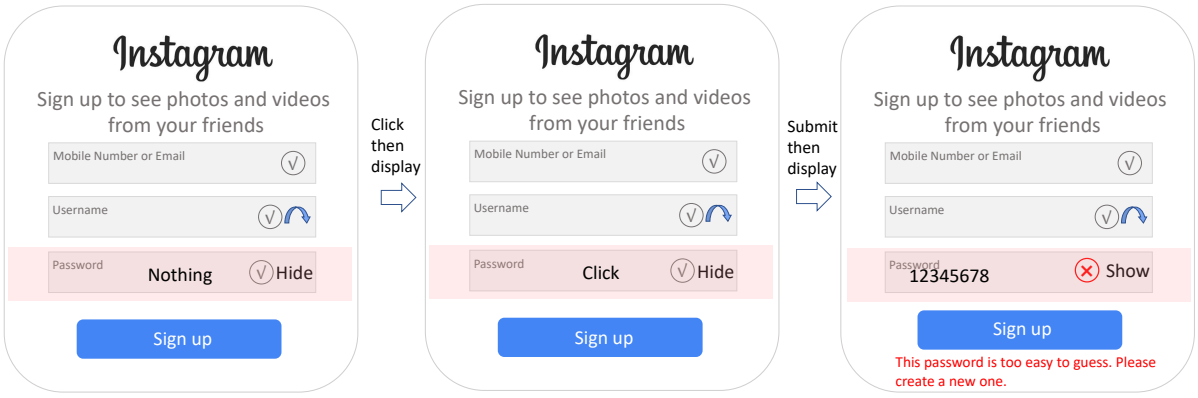


Figure F11 Password registration error message without clear password rule requirements: The website merely indicates that the registration requirements are not met without showing the exact password rules.

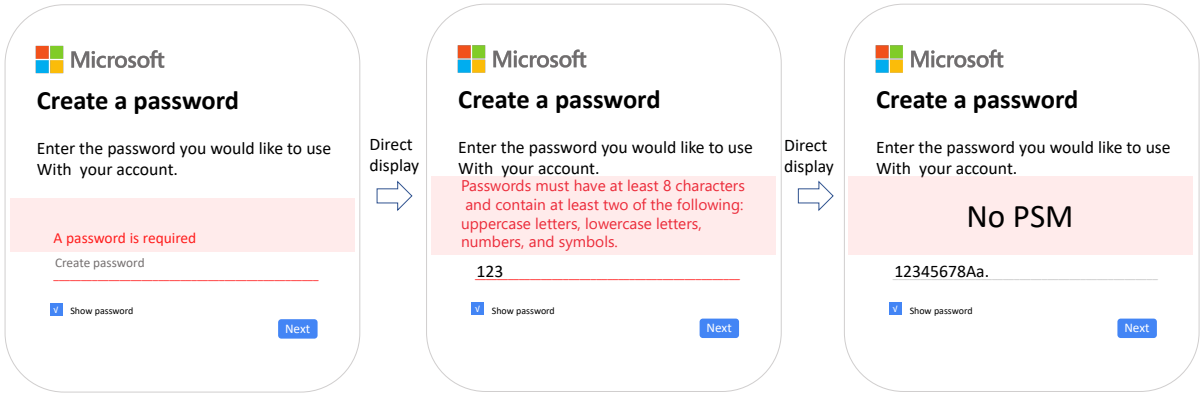


Figure F12 **No password strength meter:** The website does not provide feedback on the strength of the user-designed password.

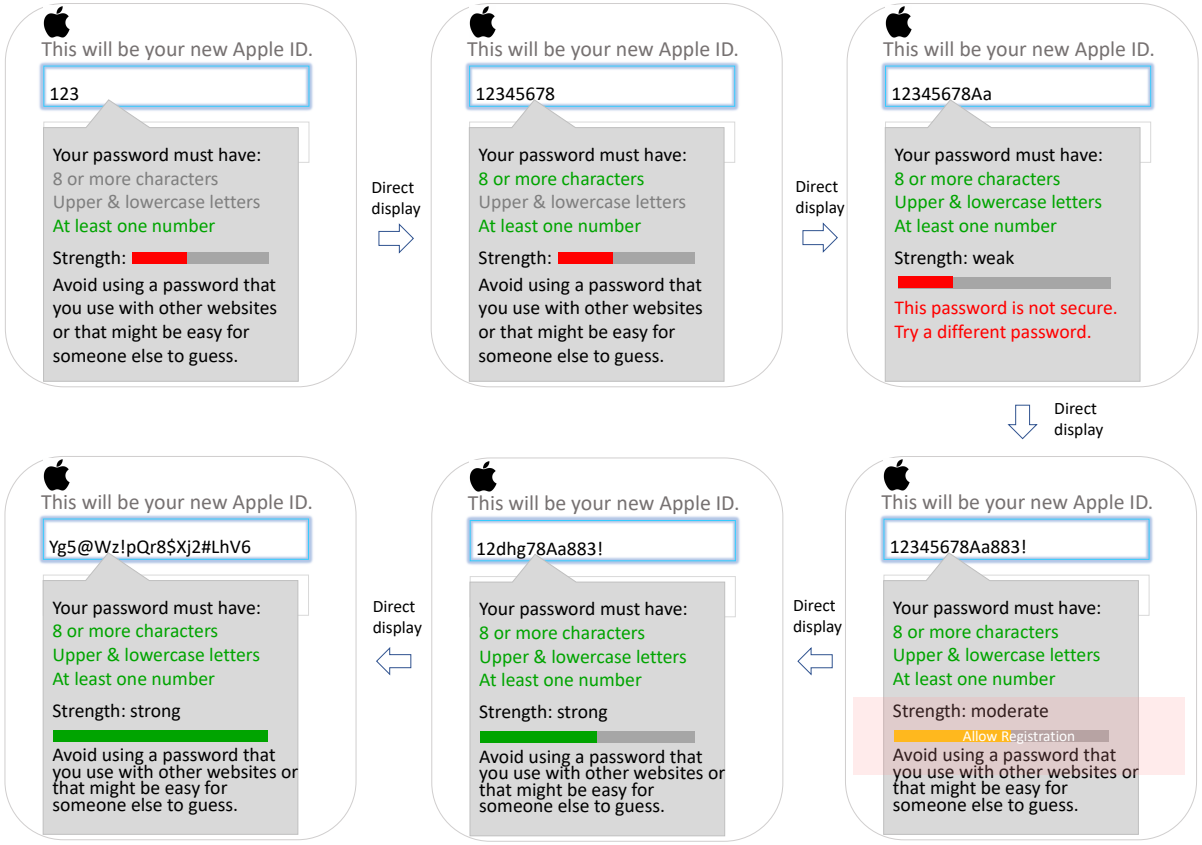


Figure F13 **Password strength feedback with text explanation and rule display:** The website provides feedback on password strength, including textual explanations and a display of password rules.

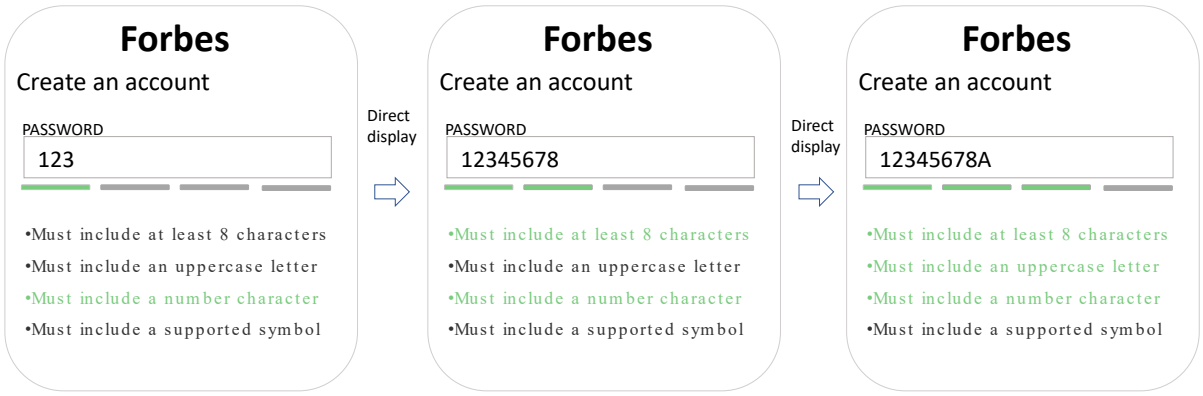


Figure F14 Password strength feedback with direct rule correlation: The website provides feedback on password strength, directly correlating each aspect of the strength indicator with specific password rule requirements. The website defines password strength based on provided rules, increasing the strength level each time a condition is met. When all conditions are satisfied, the password strength is at maximum.

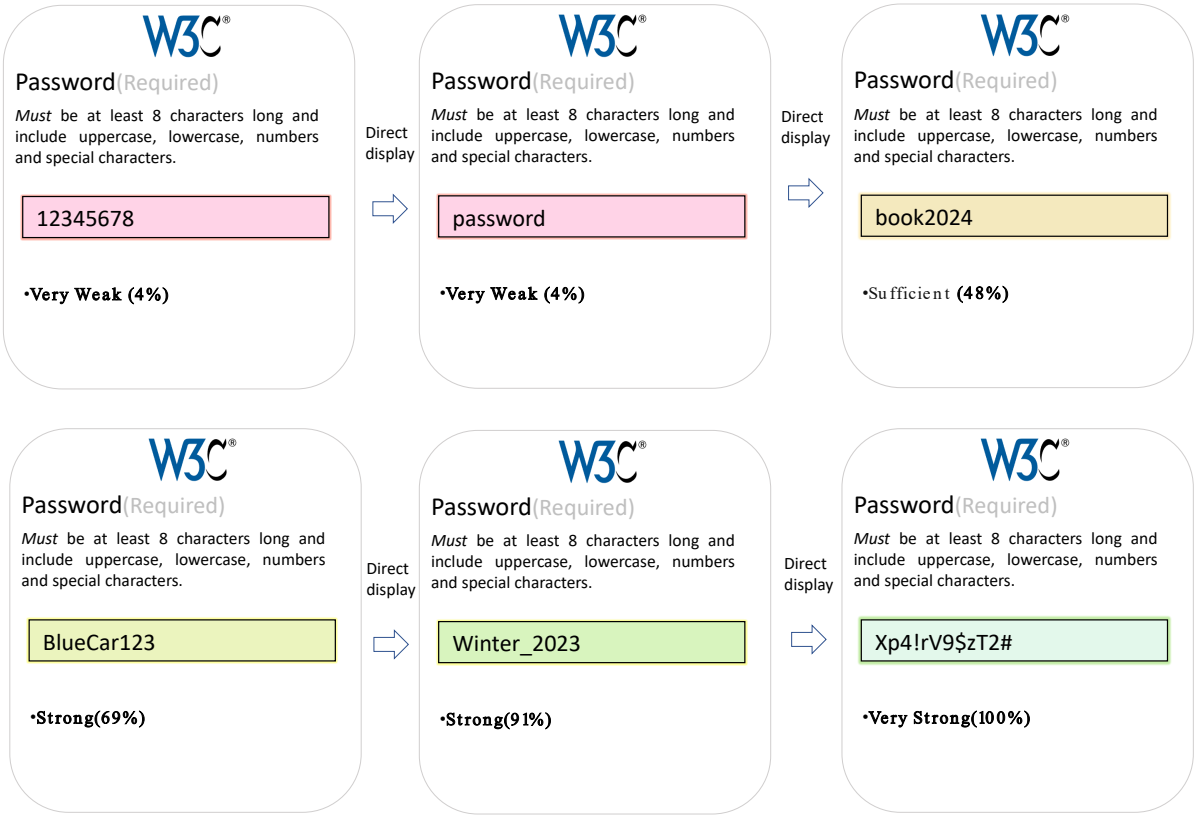


Figure F15 Password strength meter without textual explanation: The website evaluates password strengths based on different inputs and indicates whether the password is strong or weak, without providing explanations or reasons for these assessments.