A Spoonful of Sugar?
The Impact of Guidance and Feedback on Password-creation Behavior

Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Alain Forget, Saranga Komanduri, Michelle L. Mazeurek, William Melicher, Sean M. Segreti, Blase Ur
테이크어반 강남점을 이용해주셔서
대단히 감사드립니다!
※Wifi 비밀번호: 12345678
주문번호: 6
테이크어반 감녕점을 이용해주셔서

대단히 감사드립니다!

※ WiFi 비밀번호 : 12345678

주문번호: 6
Password Breaches Remain A Threat
Password Breaches Remain A Threat
Password-Composition Policies
Password-Composition Policies

• Your password must...
  • ...contain 12 or more characters
  • ...contain at least 3 of the following character classes:
    {lowercase letters, uppercase letters, digits, symbols}

---

Password-Composition Policies

• Your password must...
  • ...contain 12 or more characters
  • ...contain at least 3 of the following character classes: {lowercase letters, uppercase letters, digits, symbols}
  • ...not contain a blacklisted substring (e.g., “1234”)

Password-Composition Policies

• Your password must...
  • ...contain 12 or more characters
  • ...contain at least 3 of the following character classes: {lowercase letters, uppercase letters, digits, symbols}
  • ...not contain a blacklisted substring (e.g., “1234”)
  • ...start and end with a lowercase letter (pattern)

Can we make the creation of secure passwords more usable?
Requirements Feedback
Requirements Feedback

username2study

Please use: 8 to 32 characters, upper and lowercase letters, numbers

show
Requirements Feedback

username2study

Please use: 8 to 32 characters, Upper and lowercase letters, Numbers

✓ 8 to 32 characters
✓ Numbers
Requirements Feedback

username2study

@yahoocom

Please use: 8 to 32 characters, Upper and lowercase letters, Numbers
Requirements Feedback

username2study

Please use: ✓ 8 to 32 characters ✓ Upper and lowercase letters ✓ Numbers

✓ Upper and lowercase letters
Multi-Step Password Guidance
Multi-Step Password Guidance

pass12word
Multi-Step Password Guidance

pass12word
Multi-Step Password Guidance

pa$ss12wo!rd
Primary Research Questions
1. How do blacklist and pattern requirements impact password security and usability?
Primary Research Questions

1. How do blacklist and pattern requirements impact password security and usability?

2. Does real-time requirements feedback improve the usability of creating strong passwords?
Primary Research Questions

1. How do blacklist and pattern requirements impact password security and usability?

2. Does real-time requirements feedback improve the usability of creating strong passwords?

3. Does a multi-step guidance process improve the usability of creating strong passwords?
Methodology

• 6,435-participant online study
  • Recruited U.S. users of Amazon’s Mechanical Turk
Methodology

• 6,435-participant online study
  • Recruited U.S. users of Amazon’s Mechanical Turk

• Between-subjects design with 9 conditions
Methodology

• 6,435-participant online study
  • Recruited U.S. users of Amazon’s Mechanical Turk

• Between-subjects design with 9 conditions

• 2-part study, 2+ days apart
  • Compensated $0.55 and $0.70, respectively
  • Mazurek et al. CCS ‘13 and Fahl et al. SOUPS ‘13
Methodology

• Part 1: Create password & take survey
  • Scenario: Email provider requires password change
Methodology

• Part 1: Create password & take survey
  • Scenario: Email provider requires password change

• Part 2: Return, re-enter password, & take survey
Security Metric: Guessability

- Guessability – how many guesses to crack?
- Threat model: offline attack
Security Metric: Guessability

• Guessability – how many guesses to crack?
  • Threat model: offline attack
    • Naïve first guesses: aaaaaaaaaaaaaa, aaaaaaaaaaaab
Security Metric: Guessability

• Guessability – how many guesses to crack?
  • Threat model: offline attack
    • Naïve first guesses: $aaaaaaaaaaa, aaaaaaaaaaab$
    • Better first guesses: 123456781234, password1234
Security Metric: Guessability

• Guessability – how many guesses to crack?
  • Threat model: offline attack
    • Naïve first guesses: `aaaaaaaaaaaaaa, aaaaaaaaaaaab`
    • Better first guesses: `123456781234, password1234`

• 20 trillion guesses per condition
Usability Metrics
Usability Metrics

- Password creation
  - Time
  - # failed attempts

Image Creative Commons on Flickr by *ilahi*
Usability Metrics

• Password creation
  • Time
  • # failed attempts
• Participant sentiment
  • Self-reported
  • Study drop-out
Usability Metrics

- Password creation
  - Time
  - # failed attempts
- Participant sentiment
  - Self-reported
  - Study drop-out
- Memorability
  - ~5 minutes after creation
  - 2-5 days after creation
Usability Metrics

- Password creation
  - Time
  - # failed attempts
- Participant sentiment
  - Self-reported
  - Study drop-out
- Memorability
  - ~5 minutes after creation
  - 2-5 days after creation
- Writing down/storing password
Participants

- 6,435 participants
- 47% male, 53% female
- Median age 28
Primary Research Questions

1. How do blacklist and pattern requirements impact password security and usability?

2. Does real-time requirements feedback improve the usability of creating strong passwords?

3. Does a multi-step guidance process improve the usability of creating strong passwords?
RQ1 Conditions

• **Base**: 12+ characters from 3+ classes
RQ1 Conditions

- **Base**: 12+ characters from 3+ classes

- **Blacklist**: Base + disallowed 41,329 substrings (e.g., “1234”, years, “abcd”)
RQ1 Conditions

- **Base:** 12+ characters from 3+ classes

- **Blacklist:** Base + disallowed 41,329 substrings (e.g., “1234”, years, “abcd”)

- **Pattern:** Base + start and end w/ lowercase letter
RQ1 Results – Security

![Graph showing the relationship between number of guesses and percent guessed.](image)
RQ1 Results – Security

Percent Gussed

0% 10% 20% 30%

# Guesses

$10^3$ $10^6$ $10^9$ $10^{12}$
RQ1 Results – Security

Better
RQ1 Results – Security

Better
RQ1 Results – Security

Better
RQ1 Results – Security

Better

base

blacklist

pattern
RQ1 Results – Security

Better

Percent Gussed

# Guesses

base

blacklist

pattern
RQ1 Results – Security

Better

base

blacklist

pattern
RQ1 Results – Security

Pattern more secure than blacklist. Both are more secure than base.
RQ1 Results – Usability
RQ1 Results – Usability

- *Pattern* took longer to create than *blacklist*; *blacklist* longer than *base*
RQ1 Results – Usability

- *Pattern* took longer to create than *blacklist*; *blacklist* longer than *base*

- *Pattern* more difficult to create than *base/blacklist*
RQ1 Results – Usability

• *Pattern* took longer to create than *blacklist*; *blacklist* longer than *base*

• *Pattern* more difficult to create than *base/blacklist*

• *Pattern* stored or written down more than *base/blacklist*
Primary Research Questions

1. How do blacklist and pattern requirements impact password security and usability?

2. Does real-time requirements feedback improve the usability of creating strong passwords?

3. Does a multi-step guidance process improve the usability of creating strong passwords?
RQ2 Conditions

• Realtime ("rt") feedback

Password requirements:

• Include at least 12 characters (Your password contains 9 characters but 12 are required.)
• Password must both begin and end with a lowercase letter (a-z) (Your password must begin and end with a lowercase letter)
• Include at least 3 of the following: (Your password contains 2 types of characters but 3 are required.)
  o A lowercase English letter
  o An uppercase English letter
  o A digit
  o A symbol (something that is not a digit or an English letter)
RQ2 Results – Security

• Requirements feedback did not significantly impact security
RQ2 Results – Security

• Requirements feedback did not significantly impact security

• Feedback ➔ Less likely to exceed requirements
RQ2 Results – Usability
RQ2 Results – Usability

• More likely to submit compliant password with requirements feedback

• No significant impact on other usability metrics
RQ2 Results – Usability

• More likely to submit compliant password with requirements feedback

• No significant impact on other usability metrics
Primary Research Questions

1. How do blacklist and pattern requirements impact password security and usability?

2. Does real-time requirements feedback improve the usability of creating strong passwords?

3. Does a multi-step guidance process improve the usability of creating strong passwords?
RQ3 Conditions

- **Pattern-rt**: 12+ characters, 3+ character classes, start & end with lowercase letter, feedback
RQ3 Conditions

• **Pattern-rt**: 12+ characters, 3+ character classes, start & end with lowercase letter, feedback

• **Guide**: Multi-step creation process
  • Step 1: 10+ character pattern password
  • Step 2: **The user** adds 2 characters
RQ3 Conditions

- **Pattern-rt**: 12+ characters, 3+ character classes, start & end with lowercase letter, feedback

- **Guide**: Multi-step creation process
  - Step 1: 10+ character pattern password
  - Step 2: The **user** adds 2 characters

- **Insert**: Multi-step creation process
  - Step 1: 10+ character pattern password
  - Step 2: The **system** adds 2 random characters
RQ3 Results – Security
RQ3 Results – Security

Better
RQ3 Results – Security

Better
RQ3 Results – Security

Better
RQ3 Results – Security

Better
Multi-step guidance made passwords weaker.
RQ3 Results – Usability
RQ3 Results – Usability

• *Guide* and *insert* passwords less difficult to create than *pattern-rt*
RQ3 Results – Usability

- *Guide* and *insert* passwords less difficult to create than *pattern-rt*

- *Guide* and *insert* participants less likely to drop out than *pattern-rt*
RQ3 Results – Usability

• *Guide* and *insert* passwords less difficult to create than *pattern-rt*

• *Guide* and *insert* participants less likely to drop out than *pattern-rt*

• *Insert* more likely to be written down/stored than *pattern-rt*
Limitations

• Tested recall at only two points

• Passwords created for a research study
  • Mazurek et al. CCS ‘13 and Fahl et al. SOUPS ‘13

• Did not test multiple devices
Primary Research Questions

1. How do blacklist and pattern requirements impact password security and usability?

2. Does real-time requirements feedback improve the usability of creating strong passwords?

3. Does a multi-step guidance process improve the usability of creating strong passwords?
Conclusions

1. How do blacklist and pattern requirements impact password security and usability?

2. Does real-time requirements feedback improve the usability of creating strong passwords?

3. Does a multi-step guidance process improve the usability of creating strong passwords?
Conclusions

1. *Blacklist* and *pattern* requirements make passwords stronger, but reduce usability

2. Does *real-time requirements feedback* improve the usability of creating strong passwords?

3. Does a *multi-step guidance process* improve the usability of creating strong passwords?
Conclusions

1. **Blacklist and pattern** requirements make passwords stronger, but reduce usability.

2. **Real-time requirements feedback** did not have a major security or usability impact.

3. Does a **multi-step guidance process** improve the usability of creating strong passwords?
Conclusions

1. *Blacklist* and *pattern* requirements make passwords stronger, but reduce usability.

2. *Real-time requirements feedback* did not have a major security or usability impact.

3. *Multi-step guidance process* more usable, yet leads to weaker passwords.
Conclusions

1. **Blacklist** and **pattern** requirements make passwords stronger, but reduce usability

2. **Real-time requirements feedback** did not have a major security or usability impact

3. **Multi-step guidance process** more usable, yet leads to weaker passwords

Richard Shay, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Alain Forget, Saranga Komanduri, Michelle L. Mazurek, William Melicher, Sean M. Segreti, Blase Ur

blase@blaseur.com