

# Password Creation in the Presence of Blacklists

Hana Habib and Jessica Colnago  
Carnegie Mellon University

William Melicher, Blase Ur, Sean Segreti,  
Lujo Bauer, Nicolas Christin, and Lorrie Cranor



**Carnegie Mellon University**

# Do blacklists lead to stronger passwords?

Password

Strength



This password is too common.

Password

Strength

# Apparently, yes

## **Weir et al. CCS '10**

- Removing blacklisted passwords from sets of passwords increases strength

## **Kelley et al. IEEE SP '12**

- Bigger and complex blacklists are better

## **Shay et al. CHI '15**

- Blacklists increase security less than forcing a pattern
- Blacklists led to an increase in security with better usability

# DRAFT NIST Special Publication 800-63B

## Digital Identity Guidelines - Authentication & Lifecycle Management

- Different assurances levels
- Moving toward multi-factor authentication

## For memorized secrets (i.e. passwords)

- Do not require password complexity
- Use blacklists



**Blacklists may be helpful, but are they enough?**

**How do users react to blacklists?**

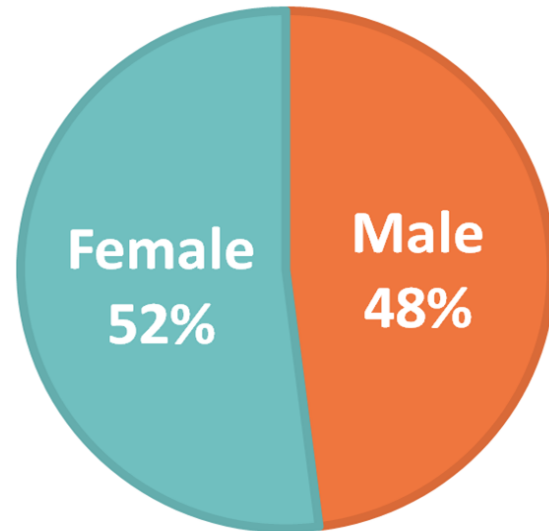
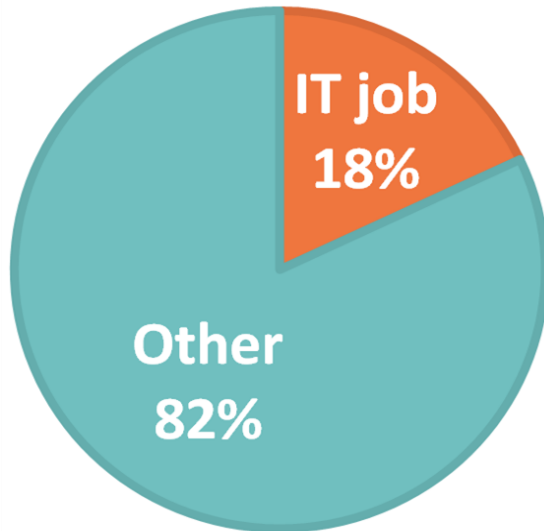
**Can we help them improve their passwords?**

# Methodology

# 2,280 participants created passwords

Mechanical Turk, ages 18+ in the U.S.

Collected for Ur et al. CHI '17



# Requirement: Not one of 96,480 passwords

**Create Your Password**

Username  
user

Password  
.....

Show Password

**Continue**

Don't reuse a password from another account! [\(Why?\)](#)

Your password must:

- ✓ Contain 8+ characters
- Not be an extremely common password

[How to make strong passwords](#)



# Condition 1: No text feedback

## Create Your Password

Username  
user

Password  
thisisastrongpassword

Show Password

Confirm Password

[Continue](#)

Don't reuse a password from another account! [\(Why?\)](#)

Your password must:

- ✓ Contain 8+ characters

[How to make strong passwords](#)

# Condition 2: Text feedback

## Create Your Password

Username  
user

Password  
thisisastrongpassword

Show Password & Detailed Feedback

Confirm Password

[Continue](#)

Your password is pretty good. Use it only for this account. [\(Why?\)](#)

To make it even better:

- Don't use common phrases (**isastrong**) or dictionary words (**password** and **this**) [\(Why?\)](#)
- Avoid using very common passwords like **password** as part of your own password [\(Why?\)](#)
- Consider using 1 or more symbols [\(Why?\)](#)

A better choice:  
**thisisastrongpasswordSD**

[How to make strong passwords](#)

# Participant groupings

## No blacklisted passwords

1,930 participants, 84.7%

## With blacklisted passwords

350 participants, 15.3%

### No reuse

106, 30.3%

Birthday → BunkBed88

### Modified reuse

64, 18.3%

stewart7 → s1t9e9w8art

### Exact reuse

180, 51.4%

happyday → happyday!

# Research questions

1. How does the strength of the final password differ between groups?
2. How do blacklisted passwords differ from final passwords?
3. What is the impact of text feedback on password strength?
4. What impact does a blacklist have on password creation sentiment?

# Results

# No blacklisted attempt → More complex passwords

A B C D E F G  
H I J K L M N  
O P Q R S T  
U V W X Y Z

1.7 x as many  
capital letters

! @ # \$ %  
^ & \* ( ) \_  
{ } - + = ? ;

1.4 x as many  
symbols

1 2 3 4 5  
6 7 8 9 0

1.1 x as many  
digits

# Notification increases complexity

A B C D E F G  
H I J K L M N  
O P Q R S T  
U V W X Y Z

**3 x as many  
capital letters**

! @ # \$ %  
^ & \* ( ) \_  
{ } - + = ? ;

**28 x as many  
symbols**

1 2 3 4 5  
6 7 8 9 0

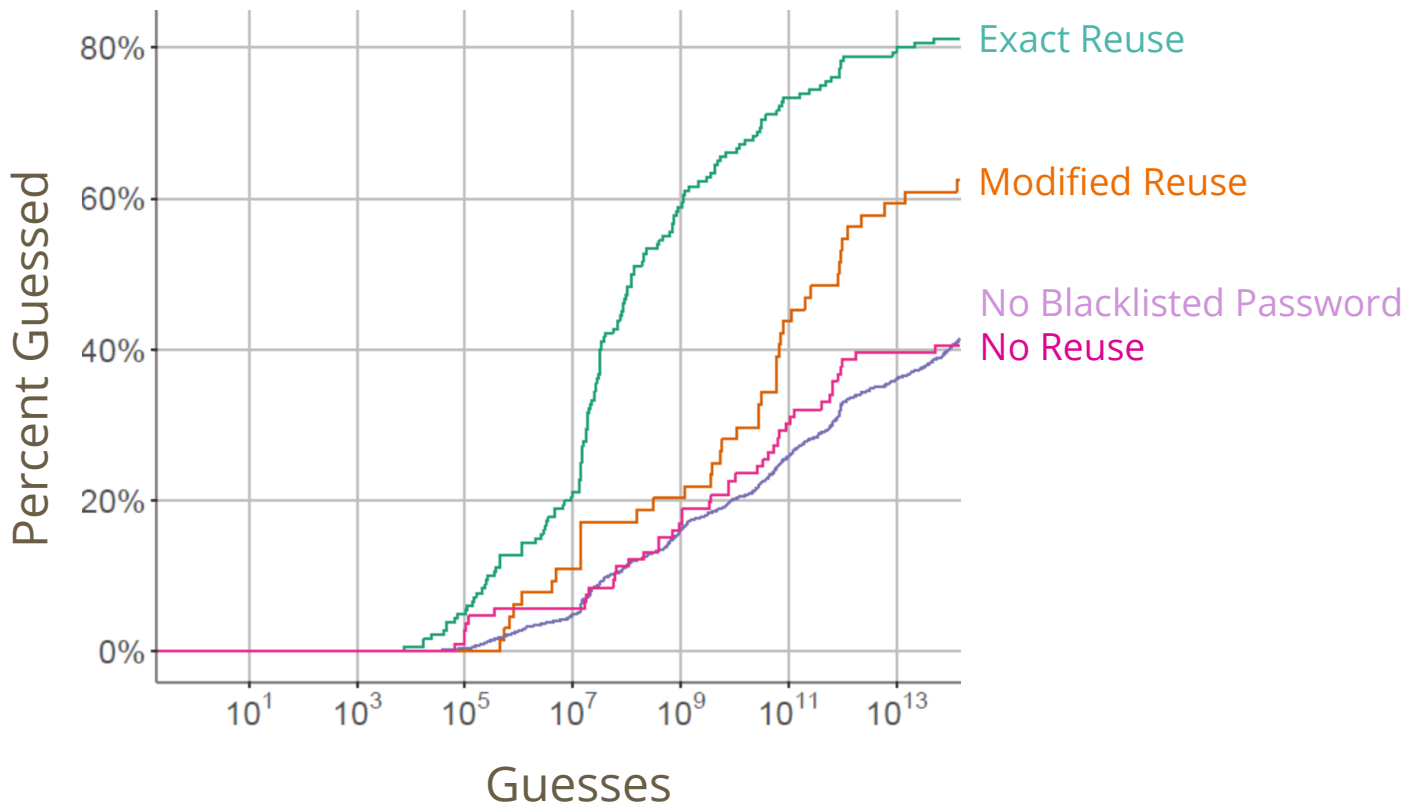
**2.3 x as many  
digits**

# People change passwords in simple ways

|                      | <b>% of Reuse Participants</b> | <b>Modified Reuse</b> | <b>Exact Reuse</b> |
|----------------------|--------------------------------|-----------------------|--------------------|
| <b>Added Digits</b>  | 92%                            | pass1word             | password1          |
| <b>Added Symbols</b> | 36%                            | pass_word             | password_          |
| <b>Added Words</b>   | 24%                            | passmyword            | passwordword       |



# Modifications → Stronger passwords



# Feedback helps with complexity

A B C D E F G  
H I J K L M N  
O P Q R S T  
U V W X Y Z

1.5 x as many  
capital letters

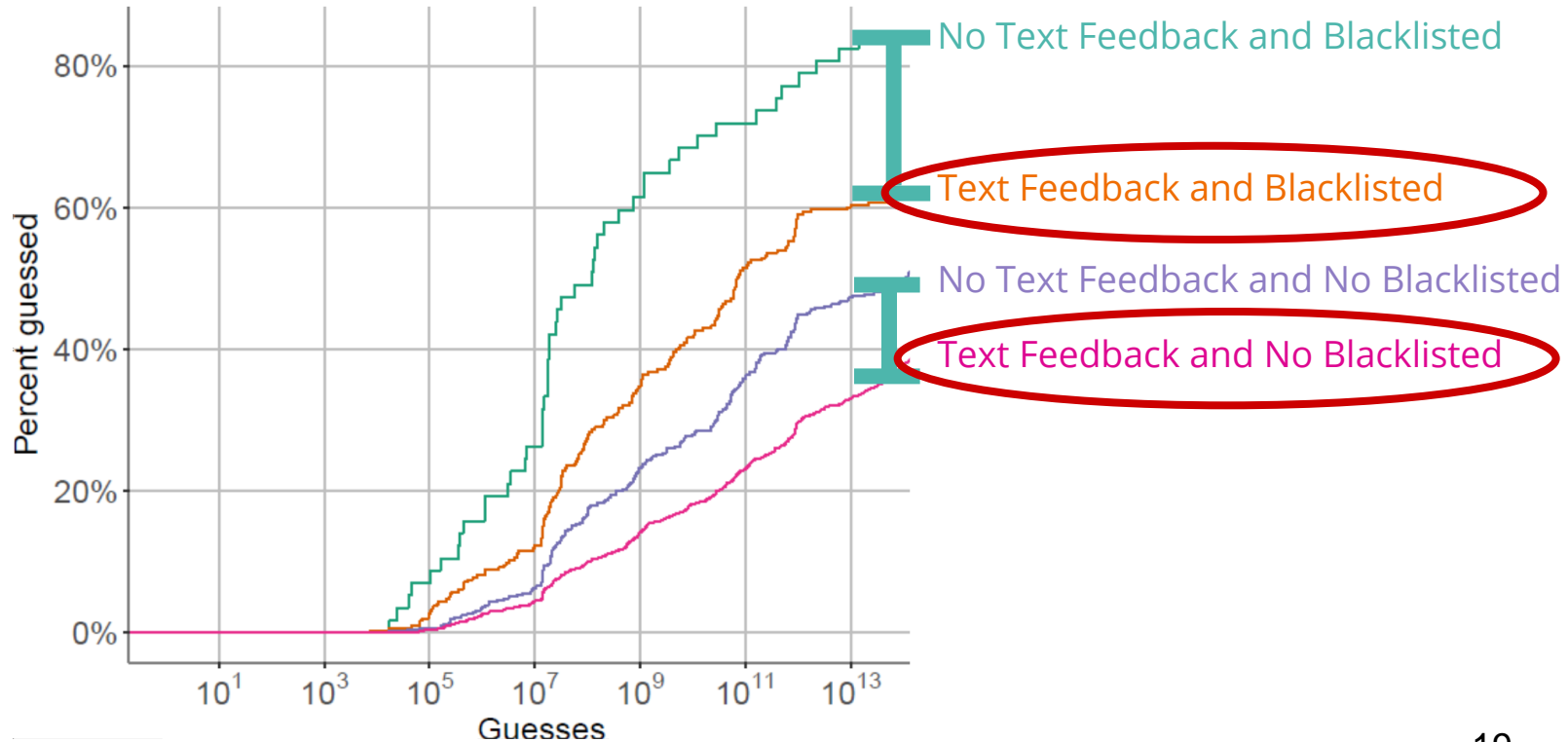
! @ # \$ %  
^ & \* ( ) \_  
{ } - + = ? ;

1.6 x as many  
symbols

1 2 3 4 5  
6 7 8 9 0

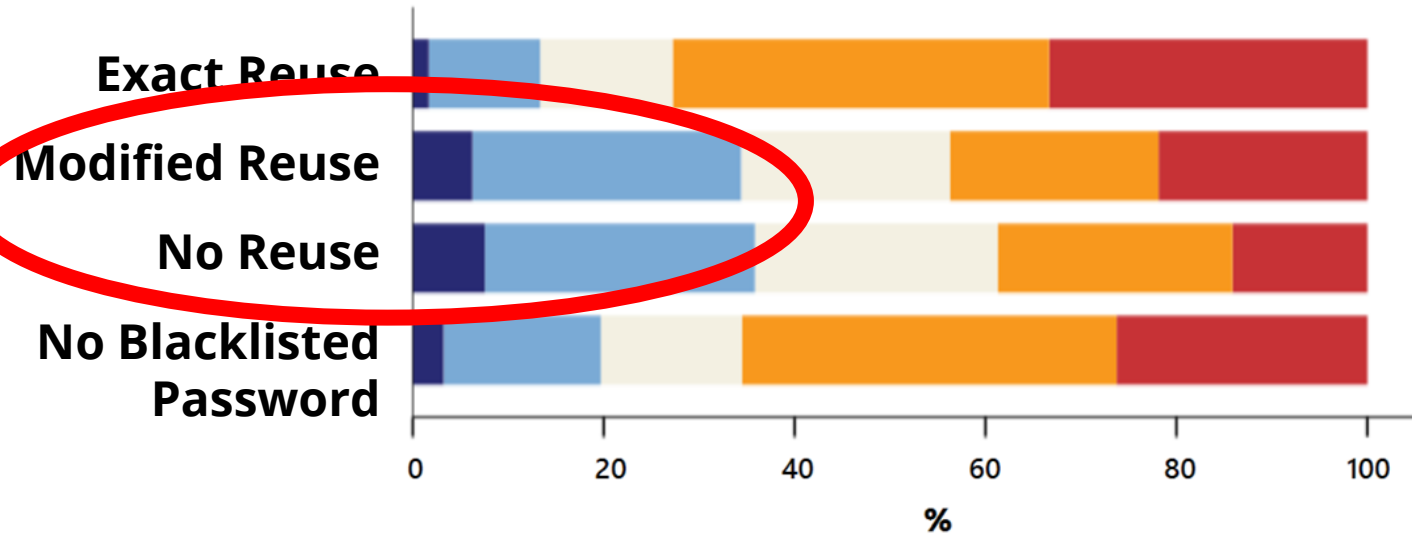
1.1 x as many  
digits

# Feedback helps with strength



# Increased effort is difficult and annoying

Difficult



Strongly agree Agree Neutral Disagree Strongly disagree

# Recommendations for your system admin

# Check for reuse of blacklisted passwords

Perform substring check

Strip out digits & symbols

~~PASSWORD~~

~~PASSWORD!~~

~~123PASSWORD!~~

US3CS4ND!3G0.17



# Provide text feedback

Your password is pretty good. Use it only for this account. [\(Why?\)](#)

To make it even better:

- Don't use common phrases (**isastrong**) or dictionary words (**password** and **this**) [\(Why?\)](#)
- Avoid using very common passwords like **password** as part of your own password [\(Why?\)](#)
- Consider using 1 or more symbols [\(Why?\)](#)

A better choice:

**thisisastrongpassword****SD**

[How to make strong passwords](#)

# Password Creation in the Presence of Blacklists

Hana Habib and Jessica Colnago, William Melicher, Blase Ur, Sean Segreti,  
Lujó Bauer, Nicolas Christin, and Lorrie Cranor

For more on this:

[ups.cs.cmu.edu/passwords/](https://ups.cs.cmu.edu/passwords/)