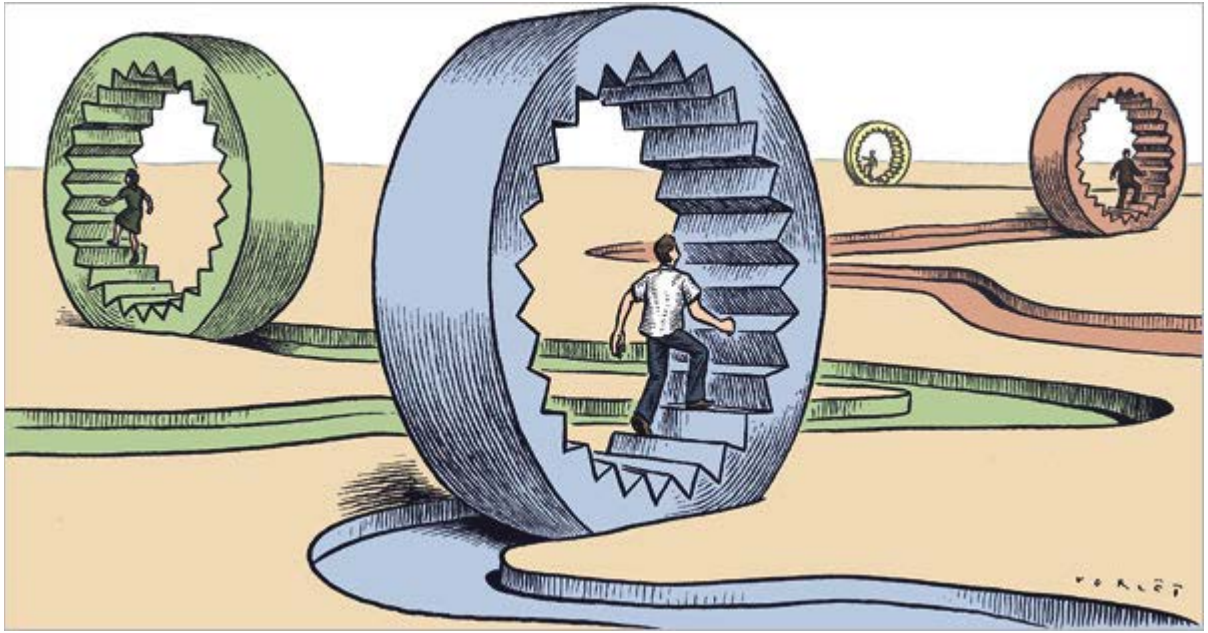
Human Behavior in Reaction to Password Security Policies

Hana Habib
htq@cs.cmu.edu

People are creatures of habit



Source: http://www.fulfilleddestiny-s3.com/blog/self-light/creatures-of-habit-part-2

How does human behavior impact the effectiveness of...

1. password expiration policies?
2. password blacklists?

Reactions to Password Expiration

First, a history lesson...

Do expiration policies help improve security?

- No protection from modern password guessing attacks
- Attackers can use password history to launch better attacks (Zhang et al. CCS'10)

Not much!

"Why do we have to change our passwords? It's not like anyone could ever guess it"

What happens when people are forced to change their passwords?

Do users make weaker passwords?

Do they have a harder time using their passwords?

Do they have negative sentiments toward their policies?

How important do they view password expiration?

Conducted 2 Mechanical Turk surveys

- Total of 695 participants
- 55% had an expiration policy
- Survey contained questions about:
  - Creating, updating, and using their main workplace password
  - Perceived relative importance of password management behaviors

What do people do to update their passwords?

	% of Participants
Modified their current password	67%
Created a new password	24%
Reused a password from another account	10%

What do people do to update their passwords?

- Applied one or two simple modifications to their password
  - 30% capitalized a letter

- Use the same strategy they used to create their passwords, e.g.,
  - Password generator
  - Substituting letters with symbols

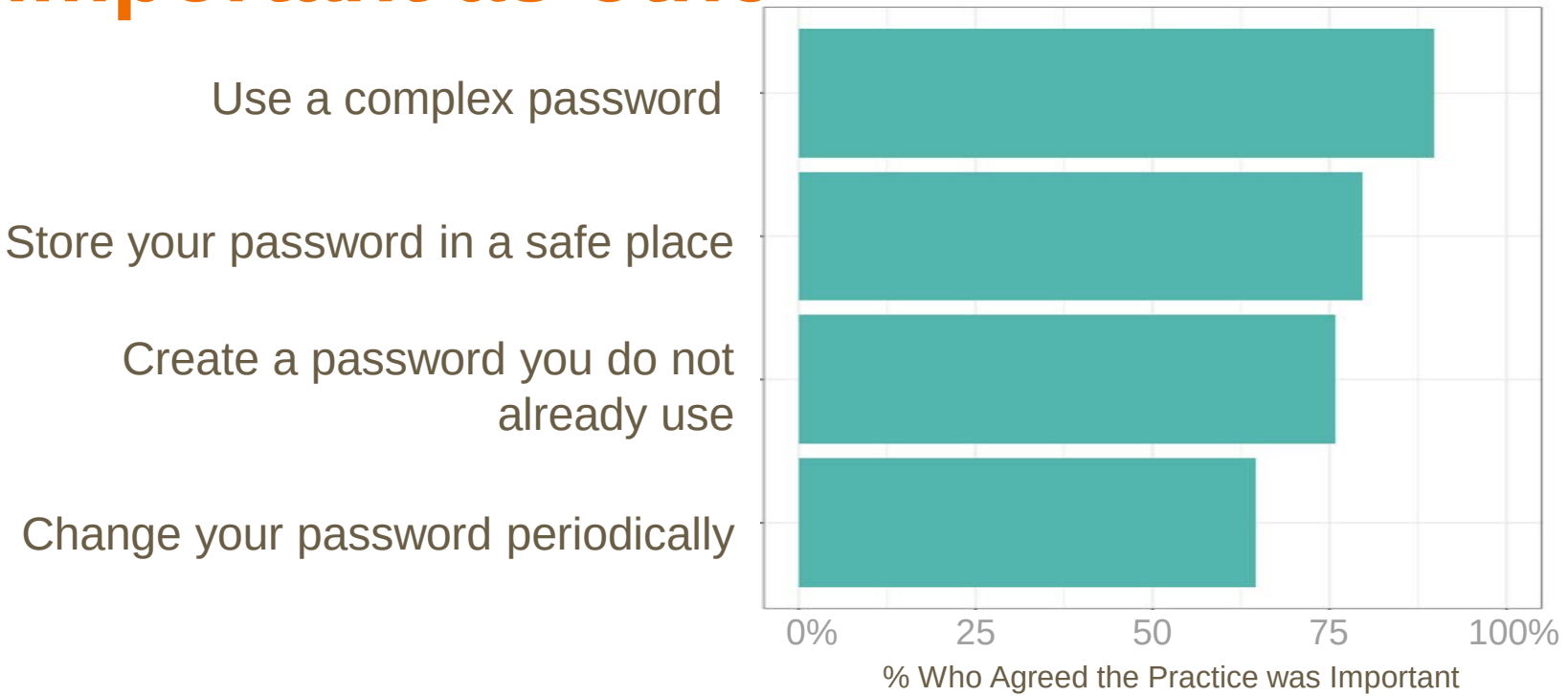
- Find a new fast food receipt

Expiration frequency had minor impact on usage

- **No influence on:**
  - Update strategies
  - Account lockouts
  - Similarity with other passwords
  - Sentiments about expiration

- **Slight influence on:**
  - Password memorization

Expiration is important...but not as important as others



Downsides of Expiration

- Inconvenient
- Insecure
- Unusable
- Ineffective

People accept the advice they’re told

- About 50% would continue changing their password if their expiration policy was removed

- **Reasons:**
  - Habit
  - Beneficial to security

Expiration does not lead to weaker passwords or negative reactions...

BUT

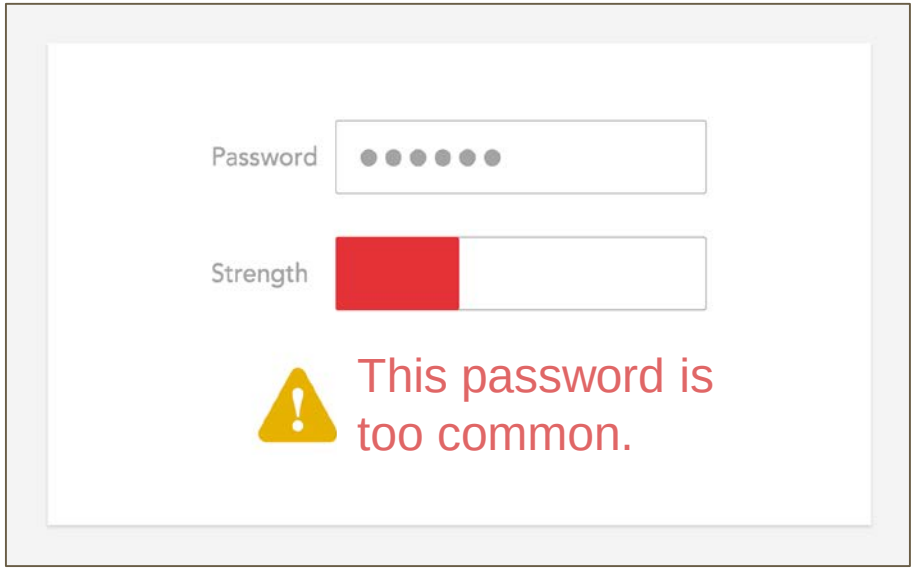
...people have developed coping mechanisms which harm security

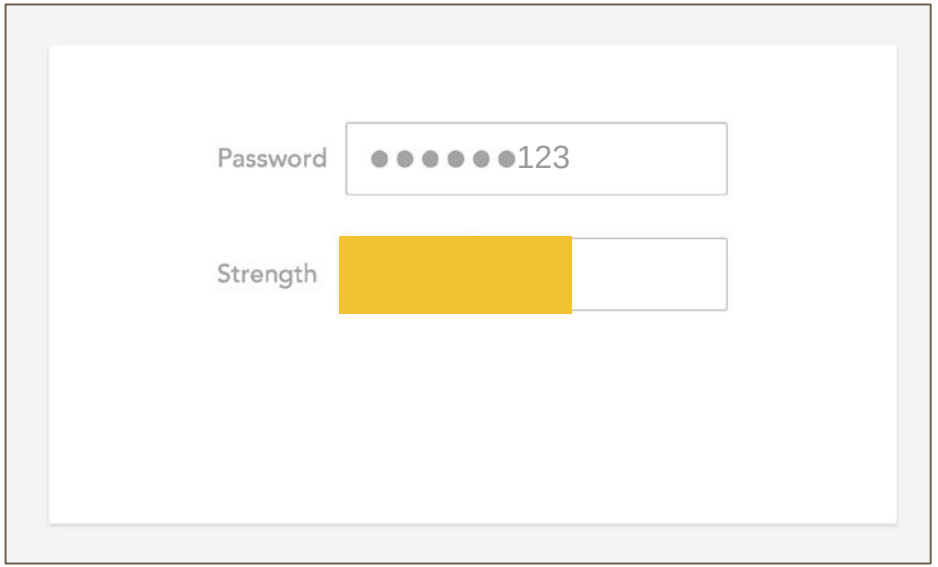
Password Creation in the Presence of Blacklists

Presented at USEC'17

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

Do blacklists lead to stronger passwords?





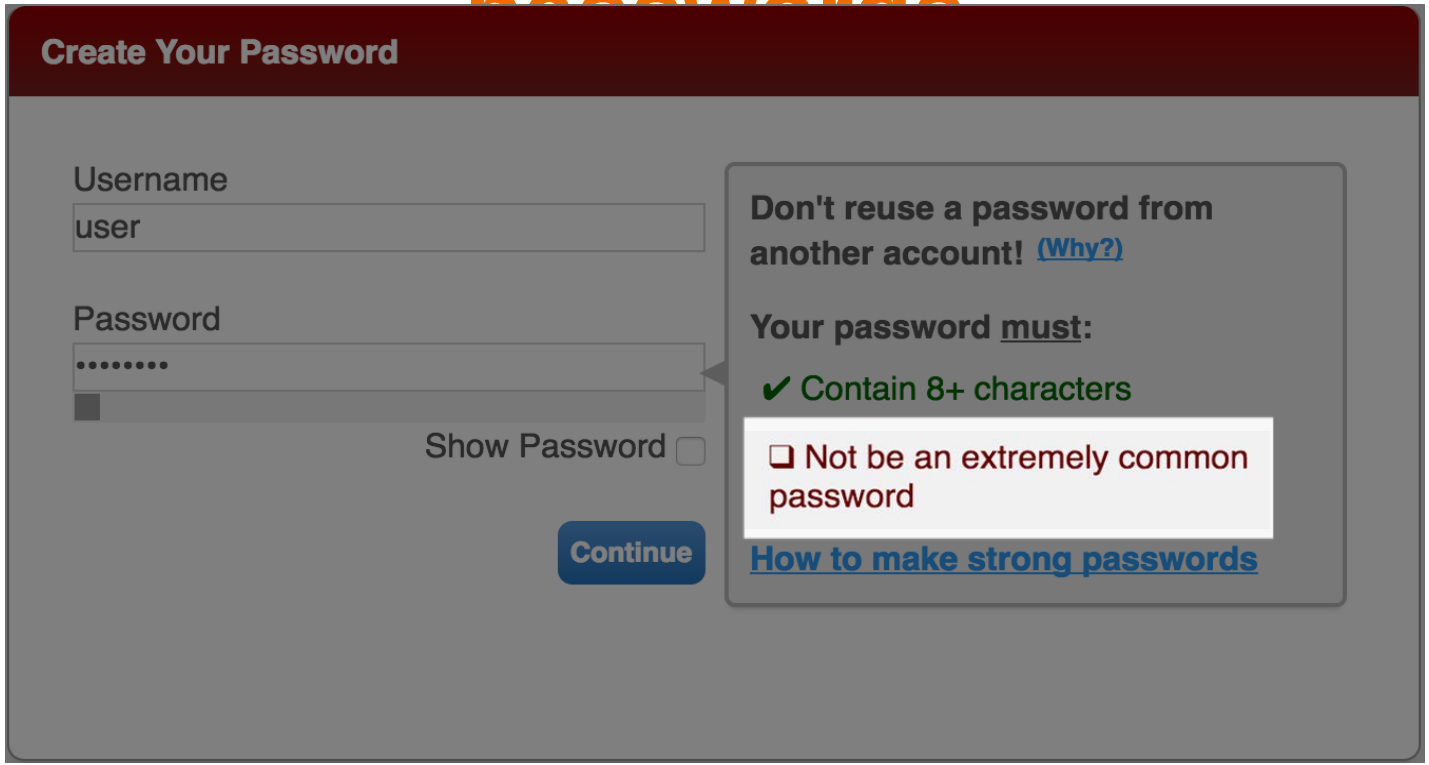
Prior work has found that blacklists help with security

Blacklists may be helpful, but are they enough?

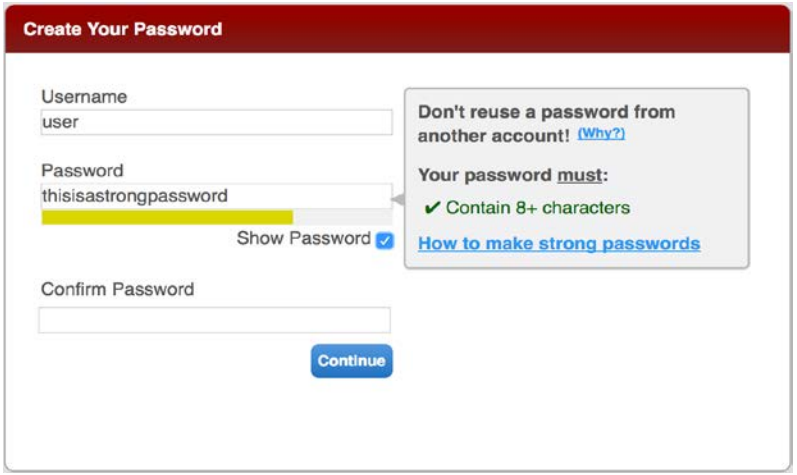
How do users react to blacklists?

Can we help them improve their passwords?

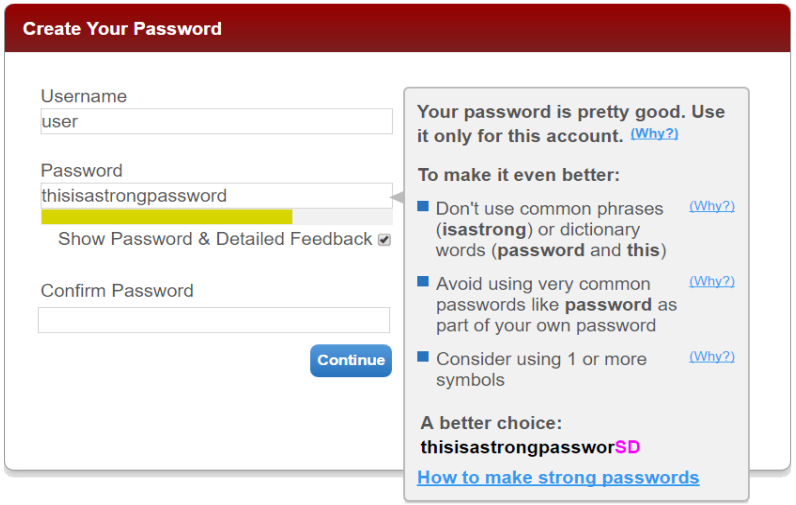
Requirement: Not one of 96,480 passwords



Two Feedback Conditions



No Text Feedback



With Text Feedback

Participant groupings

No blacklisted passwords
1,930 participants, 84.7%

With blacklisted passwords
350 participants, 15.3%

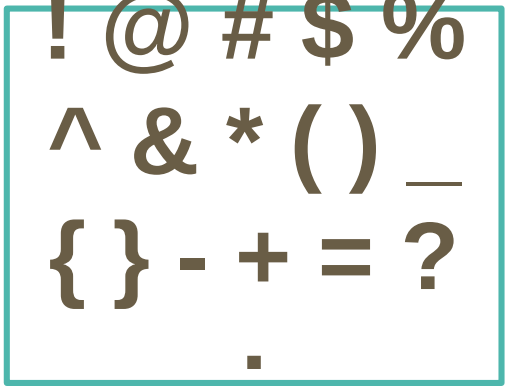
No reuse
106, 30.3%
Birthday → BunkBed88

Modified reuse
64, 18.3%
stewart7→ s1t9e9w8art

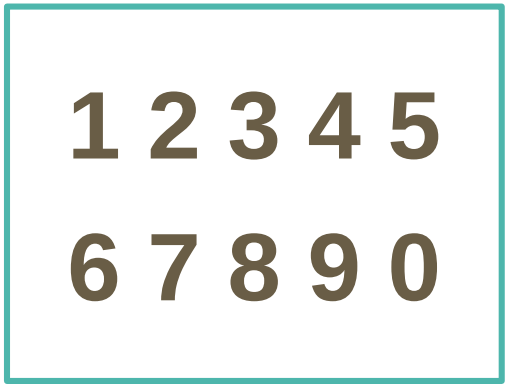
Exact reuse
180, 51.4%
happyday → happyday!

No blacklisted attempt → More complex passwords

1.7 x as many capital letters



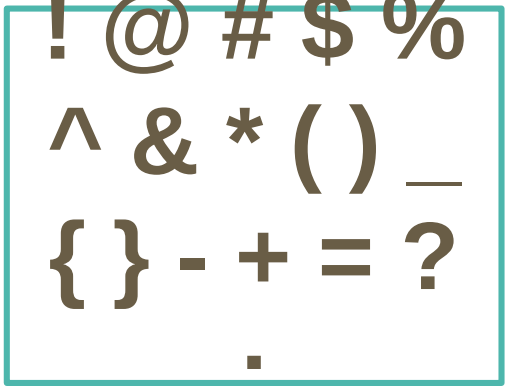
1.4 x as many symbols



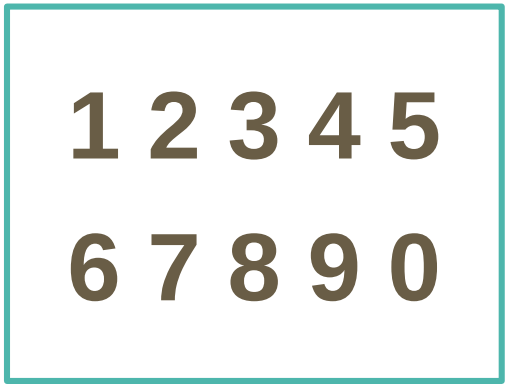
1.1 x as many digits

Notification increases complexity

3 x as many capital letters



28 x as many symbols

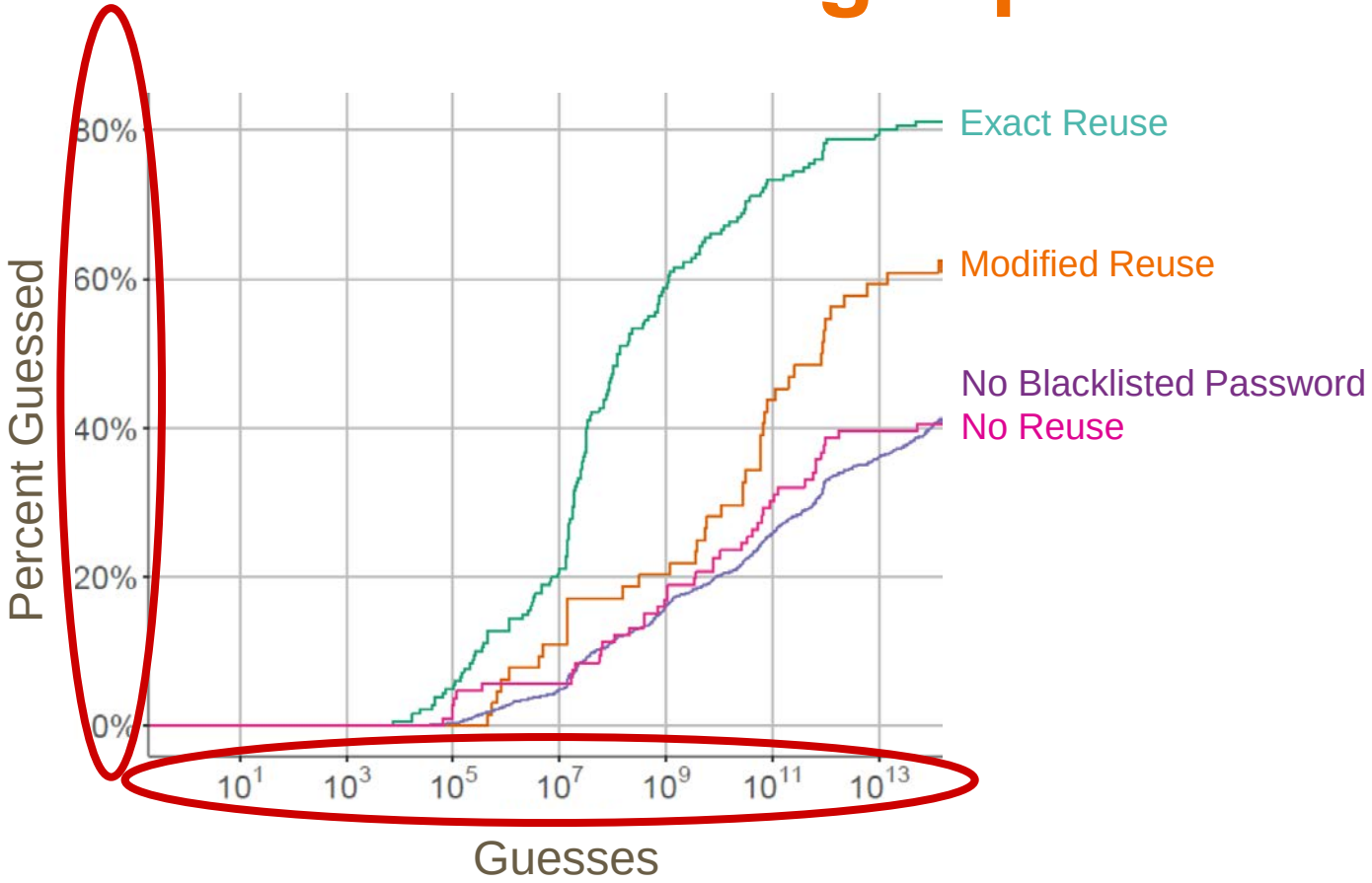


2.3 x as many digits

People change passwords in simple ways

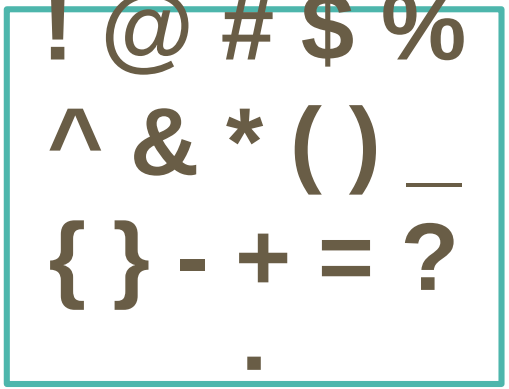
	% of Reuse Participants	Modified Reuse	Exact Reuse
Added Digits	92%	pass1word	password1
Added Symbols	36%	pass_word	password_
Added Words	24%	passmyword	passwordword

Modifications → Stronger passwords

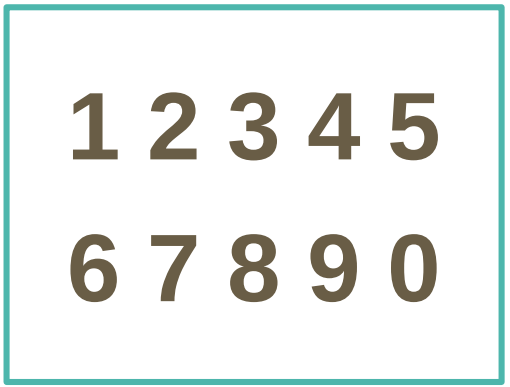


Feedback helps with complexity

1.5 x as many capital letters

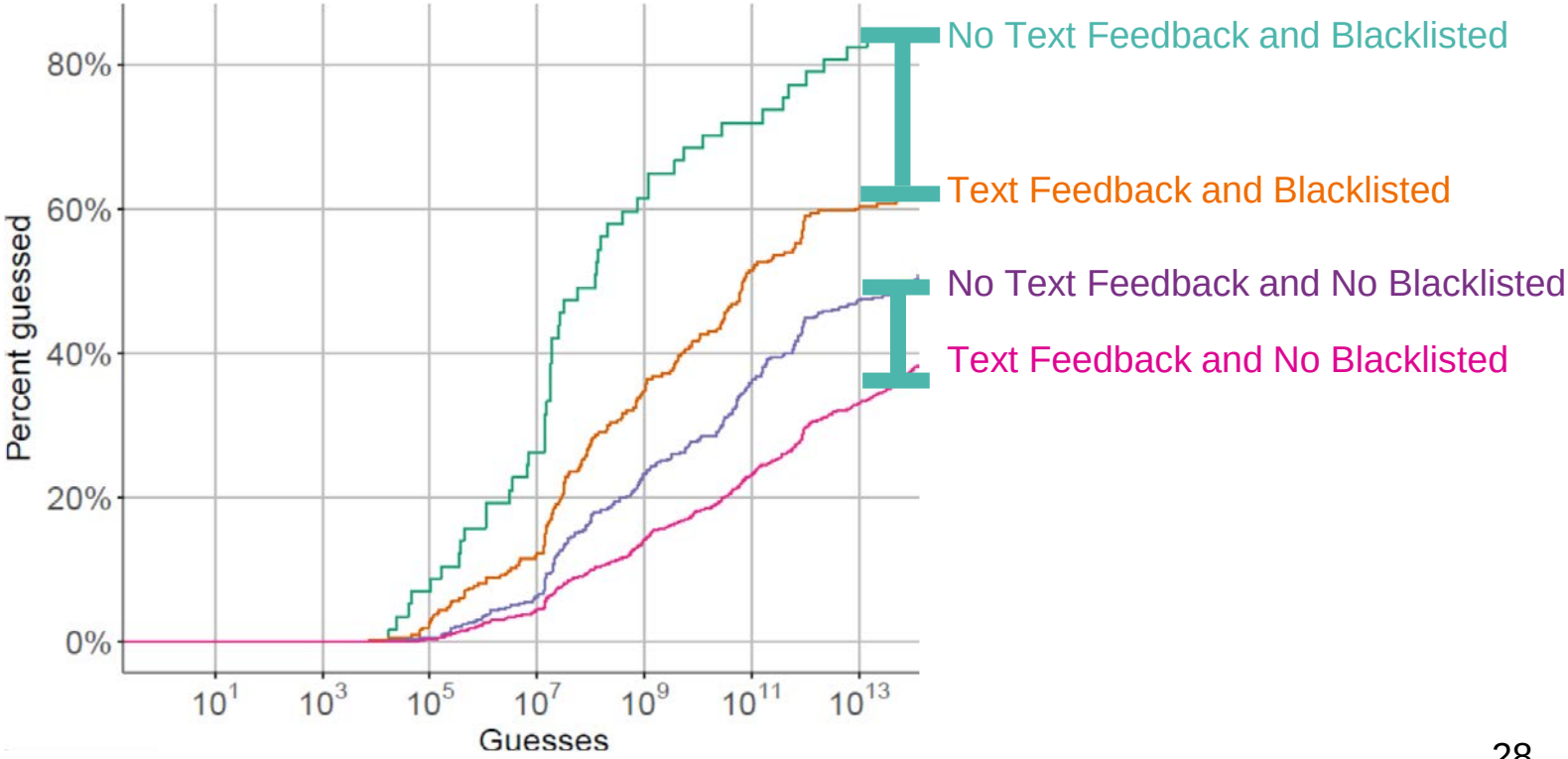


1.6 x as many symbols



1.1 x as many digits

Feedback helps with strength



Recommendations for your system admin

Enable users to create & manage complex passwords

- Expiration doesn’t inspire people to create complex passwords
- Breached passwords can be used to improve attacks

Source: https://support.managed.com/kb/a2245/best-practice-strong-password-policy.aspx

Check for reuse of blacklisted passwords

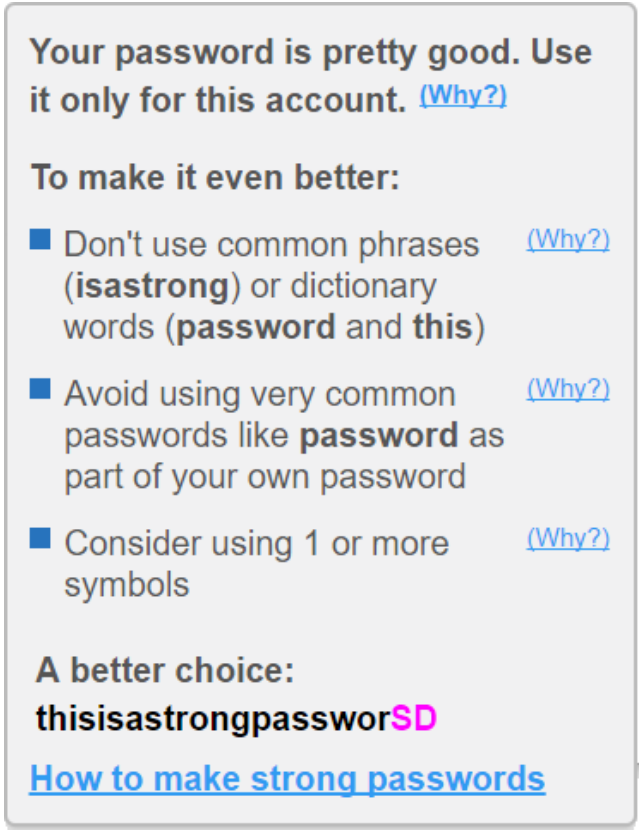
~~password~~

~~password!~~

~~123password!~~

C2y^l#a/b!1

Provide text feedback



For more on this:
cups.cs.cmu.edu/passwords/