Design and Evaluation of a Data-Driven Password Meter

Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, William Melicher
Password Meters Are Ubiquitous

- Brilliant
- Fair
- Weak
- Strong

Password strength: Strong

- Include at least 8 characters
- Don't use your name or email address
- Use a mix of uppercase and lowercase letters, numbers, and symbols
- Make your password hard to guess - even for a close friend
Problem 1: Inaccurate Scoring
Problem 2: Unhelpful Feedback

Please enter a stronger password.

Please enter a stronger password.
We designed & tested a meter with:
1) Principled strength estimates
2) Data-driven feedback to users
We designed & tested a meter with:

1) Principled strength estimates
2) Data-driven feedback to users
Neural Network to Estimate Strength

W. Melicher, B. Ur, S. Segreti, S. Komanduri, L. Bauer, N. Christin, L. Cranor.
Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks.

Image CC by Wes Breazell, Noun Project
We designed & tested a meter with:

1) Principled strength estimates

2) Data-driven feedback to users
Provide Intelligible Explanations

- 21 characteristics
- Weightings determined with regression

Unic0rns

Don't use simple transformations of words or phrases (unicorns → Unic0rns)

Capitalize a letter in the middle, rather than the first character
We designed & tested a meter with:
1) Principled strength estimates
2) Data-driven feedback to users
Main Screen…

Username: blase

Password: ********

Don’t reuse a password from another account! (Why?)

Your password must:
- Contain 12+ characters
- Use 3+ of the following: uppercase letters; lowercase letters; digits; symbols

How to make strong passwords
…Shows Requirements

Create Your Password

Username
blase

Password

Don't reuse a password from another account! (Why?)

Your password must:

- Use 3+ of the following: uppercase letters; lowercase letters; digits; symbols

How to make strong passwords
…Emphasizes Avoiding Reuse
…Provides Abstract Advice
After Requirements Are Met…

Username
blase

Password
************

Confirm Password

Your password could be better.
- Don’t use dictionary words or words used on Wikipedia (Why?)
- Consider inserting digits into the middle (Why?)
- Consider making your password longer (Why?)

See Your Password With Our Improvements

How to make strong passwords
...Displays Score Visually
…Provides Text Feedback

Create Your Password

Username
blase

Password

Show Password & Detailed Feedback

Continue

Your password could be better.

- Don’t use dictionary words or words used on Wikipedia (Why?)
- Consider inserting digits into the middle (Why?)
- Consider making your password longer (Why?)

See Your Password With Our Improvements

How to make strong passwords
…Gives Detail (Password Shown)
…Offers Explanations

Create Your Password

Username
blase

Password
CryptoUnicorn3|

Show Password & Detailed Feedback

Confirm Password

Your password could be better.

- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto).
  (Why?)

- Consider inserting digits into the middle, not just at the end.
  (Why?)

- Consider making your password longer than 14 characters.
  (Why?)

A better choice: CryptoUnicorn@

How to make strong passwords
Explanations Shown in Modal

A better choice: CryptoUnicorn@

Your password could be better.

- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto)
  Attackers use software that automatically guesses millions of words commonly found in dictionaries, wordlists, or other people’s passwords

- Consider inserting digits into the middle, not just at the end
  38% of people also put digits at the end of the password

- Consider making your password longer than 14 characters
  In recent years, attackers have gotten much better at guessing passwords under 16 characters

How to make strong passwords
We designed & **tested a meter** with:
1) Principled strength estimates
2) Data-driven feedback to users
Evaluation

• 2-part online study
  1) Create password; survey; recall password
     (48 hours later, send automated email)
  2) Recall password; survey

• 4,509 Mechanical Turk participants
  – Between-subjects
  – Full-factorial design along three dimensions
Dimension 1: Composition Policy

- 8+ characters (1class8)
  - password

- 12+ characters, 3+ classes (3class12)
  - Password1234
Dimension 2: Stringency

- Low
- Medium
- High
Dimension 2: Stringency

- Low \(10^4\) guesses
- Medium \(10^6\) guesses
- High \(10^8\) guesses
Dimension 2: Stringency

- Low: $10^4$ guesses, $10^8$ guesses
- Medium: $10^6$ guesses, $10^{12}$ guesses
- High: $10^8$ guesses, $10^{16}$ guesses
Dimension 3: Feedback
Create Your Password

Username
blase

Password
************

Show Password & Detailed Feedback

Confirm Password

Continue
Bar Only
Public (Non-Sensitive) Feedback

Create Your Password

Username
blase

Password
··············

Show Password & Detailed Feedback

Confirm Password

Your password could be better.
- Don’t use dictionary words or words used on Wikipedia
- Consider inserting digits into the middle
- Consider making your password longer

See Your Password With Our Improvements

How to make strong passwords
Standard Feedback

Your password could be better.

- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto)
- Consider inserting digits into the middle, not just at the end
- Consider making your password longer than 14 characters

A better choice: CRYPTOUnicorn@

How to make strong passwords
Standard Feedback

Username: blase
Password: CryptoUnicorn3|
Confirm Password: 

Your password could be better:
- Don’t use dictionary words (Unicorn) or words used on Wikipedia (Crypto)
- Consider inserting digits into the middle, not just at the end
- Consider making your password longer than 14 characters

A better choice: C3ryptoUnicorn@

How to make strong passwords
Standard Feedback
Standard, No Suggested Improvement
Standard, No Bar
Measure Password Guessability

Percent guessed

Guesses

0%

10^1 10^3 10^5 10^7 10^9 10^{11} 10^{13} 10^{15}
Measure Password Guessability

Percent guessed vs. Guesses
Measure Password Guessability
Measure Password Guessability

Passwords harder to guess

Percent guessed

Guesses

$10^1, 10^3, 10^5, 10^7, 10^9, 10^{11}, 10^{13}, 10^{15}$
Measure Password Guessability

Percent guessed

Guesses

1c8–None
Feedback → More Secure Passwords

![Graph showing percent guessed vs guesses for 1c8-None and 1c8-Bar-M.](image)
Feedback → More Secure Passwords

Percent guessed

Guesses

1c8–None
1c8–Bar–M
1c8–Std–M
Feedback → More Secure Passwords
Usability Results

• Feedback did **not** significantly impact password memorability
• More feedback $\rightarrow$ more difficult, annoying
• All features had value for some participants
Code Is Open Source

https://github.com/cupslab/password_meter

• Deploy now for policies like 1class8
• Help us improve the meter
• Demo: https://cups.cs.cmu.edu/meter

Design and Evaluation of a Data-Driven Password Meter
Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, William Melicher