MAKE PASSWORDS GREAT AGAIN

-ZXCVBN

-****
CELEBRATING 10 YEARS TOGETHER
WHICH PASSWORD IS BETTER?

bluegiraffeplaysball

Tr0ub4dor&3
What’s considered to be a good password

A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase.

- 6+ characters
- MiXed CaSE
- numb3rs
- special ch@r@cters!
# COMPARISON

<table>
<thead>
<tr>
<th></th>
<th>1st</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6+</td>
<td>🟢</td>
<td>🟢</td>
</tr>
<tr>
<td>CaSE</td>
<td>🟢</td>
<td>🟥</td>
</tr>
<tr>
<td>numb3rs</td>
<td>🟢</td>
<td>🟥</td>
</tr>
<tr>
<td>ch@r@cters</td>
<td>🟢</td>
<td>🟥</td>
</tr>
</tbody>
</table>
Open sesame!

Your username or password are incorrect.

Op3n $e$ame?
Hard to guess

Easy to remember
STRENGTH HEURISTICS

number of guesses required to find the password

entropy - # of bits it takes to represent a password

\[ ent = \log(n) \]
BRUTE FORCE HEURISTIC

\[ \text{entropy} = \text{length} \times \log(\text{cardinality}) \]

<table>
<thead>
<tr>
<th>log(cardinality)</th>
<th>abc 5</th>
<th>abc+ABC+123+@$% 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>entropy</td>
<td>vxcblt 30</td>
<td>d%ac3? 42</td>
</tr>
<tr>
<td>1000/sec.</td>
<td>15 days</td>
<td>140 years</td>
</tr>
</tbody>
</table>
We’re humans

Not robots
HARDER TO GUESS

Tr0ub4dor & 3

L33T

1000/sec.

3 days
HARDER TO GUESS

bluegiraffeplaysball

44 characters, 1000/sec. attempt rate, 550 years to guess.
EASY TO REMEMBER

Tr0mbone?3
Troubad0r?3
Tr0ubador?3
Tr0ub4d0r!3
Tr0ubad0r?3
Tr0ub4d0r&3
:0
password123456!

Password strength: Strong
Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet’s name. Why?

Create a password

Confirm your password

New

Password strength: Strong

------------------

*with uppercase P
Password to test: password123456!

Estimating strength of password "password123456!":

Approx time to crack: instant
(in seconds): 0
Strength score (1-5): 1
Entropy estimate (bits): 3

password:
  pattern: dictionary
token: password
rank: 1
entropy: 0

123456:
  pattern: dictionary
token: 123456
rank: 2
entropy: 1

!: 
  pattern: dictionary
token: !
rank: 2
l33t_entropy: 1
entropy: 2

https://www.bennish.net/password-strength-checker/
ZXCVBN - REALISTIC PASSWORD ESTIMATOR

Initiated @ hack week 2012 by Dan Wheeler

Implemented in by Daniel Wolf

Open-sourced on under MIT license

7,155 ☆ | 25 | 454

Last Python release - Jan 17’
HOW IT WORKS?
TECH PART AHEAD (~7 MIN.)

- LISTEN
- TAKE A NAP
MATCH
BREAK TO SUBSTRINGS
SCORE
SEARCH

password123456!
password123456!
password123456!
password123456!
password123456!
password123456!
password123456!
password123456!
passwordord123456!
pasword123456!
pasword123456!
pasword123456!
MATCH → SCORE

Ab

Dictionary

log(rank)

L33T

Reverse

+1

L33T

Spatial

L - L33T; T - Other;

\[ \log \left( \frac{1}{2} \sum_{i=1}^{\min(L,T)} (L+T) \right) \]

\[ \log \left( \frac{1}{2} \sum_{i=1}^{L} \sum_{j=1}^{\min(T,i-1)} (i-1)SD^j \right) \]

L - Length; T - turns; D - neighbors

Repeat

Date

123

Sequence

Brute force

log(repeat • rank)

log(365 • |2016 - year|)

log(start • length • |Δ|)

lower: 5
+upper
+numbers: 6
+symbols: 7
password123456!

password+123+456!

pass+word+123456+!
### Index

<table>
<thead>
<tr>
<th>Match</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>password (7,0)</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>18</td>
<td>24</td>
<td>30</td>
<td>36</td>
<td>43</td>
</tr>
<tr>
<td>123 (10, 3)</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>15</td>
<td>21</td>
<td>27</td>
<td>33</td>
<td>8</td>
</tr>
<tr>
<td>123456 (13,1)</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>15</td>
<td>21</td>
<td>27</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>! (14, 2)</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>0</td>
<td>6</td>
<td>12</td>
<td>15</td>
<td>21</td>
<td>27</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>pass (3,5)</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
<td>31</td>
<td>37</td>
<td>43</td>
<td>50</td>
<td>56</td>
<td>62</td>
<td>69</td>
</tr>
<tr>
<td>word (7,8)</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>13</td>
<td>19</td>
<td>25</td>
<td>31</td>
<td>37</td>
<td>43</td>
<td>49</td>
<td>56</td>
</tr>
<tr>
<td>word (index, score)</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
</tr>
</tbody>
</table>

### Match

- password (7,0)
- 123 (10, 3)
- 123456 (13,1)
- ! (14, 2)
MORE REASON TO USE “ZXCVBN”

⏰ Fast: ~5-20ms for up to 25 characters

📊 Lightweight: code:<50kb; data:<1mb;

Implemented in:  

Python  🐍  Java  ⚡  golang  ☵  Rust  ♻️  C++  🍓  JS
pip install zxcvbn-python

from zxcvbn import zxcvbn
results = zxcvbn('PyCon2017')
RESULTS

```json
{
  'crack_times_seconds': {
    'online_no_throttling_10_per_second': 100000000.1,
    'online_throttling_100_per_hour': 36000000036.0,
    'offline_fast_hashing_1e10_per_second': 0.1000000001,
    'offline_slow_hashing_1e4_per_second': 100000.0001
  },
  'feedback': {'warning': '', 'suggestions': []},
  'guesses_log10': 9.000000000434293,
  'sequence': [{
    'guesses': 1000000000,
    'guesses_log10': 8.999999999999998,
    'pattern': 'bruteforce',
    'token': 'Pycon2017'
  }],
  'score': 3,
  'password': 'Pycon2017',
  'calc_time': datetime.timedelta(0, 0, 4309)
}
```
Strength Meter: 4 levels
Not required (Only requirement - 6 chars)
Admins want to protect their users by requiring them to use strong passwords.
Password Requirement Competitor

Password Requirements

Character settings:
- Minimum required characters: 8
- Require number(s): 2
- Require special character(s): 1
- Require at least one uppercase letter
- Prevent common words / email address as a password:

Password resets:
- Require users to reset passwords every: 30 days

Perform a global password reset now.
All users and admins will be required to change their password on next login.

Reset Passwords Now

Prevent reusing passwords from: Last 4 times
PASSWORD REQUIREMENT @ Dropbox

Admin:

Password control

Password strength
Require your team to set stronger passwords on their Dropbox accounts.
User:

Your new password should be at least two bars: 🔄

Password doesn't meet the requirement. Please try again.

••••••
PROBLEMS

Compatibility:

Feedback:
Repeats like "abcabcabc" are only slightly harder to guess than "abc".
FUN PART AHEAD (~2 MIN.)

PARTY POOPER
DISCLAIMER

This is only an introduction to password estimation and “zxcvbn” library.

A lot of the details are not accurate, edge cases are ignored and corners are cut.

I made all that in order to simplify (sometimes even over-simplify) the talk, make it fun and short (20 minute).

If you find this topic interesting, please take a look on the “more info” slide, for more accurate, updated, formal and detailed information.
MORE INFO

• This xkcd inspired zxcvbn and my slides.

*I made a minor change to “bluegiraffeplaysball” because I believe it’s easier to remember ("correct" is somehow a word that is not easy to imagine), and the word order is easier (was it “batterystaple” or “staplebatter”?).

• Dan Wheeler’s blog about zxcvbn motivation, algorithm, structure
• Dan Wheeler’s talk about zxcvbn
• Dan Wheeler’s formal docs about zxcvbn
• zxcvbn main GitHub repository
CREDITS

• **XKCD creators** for their great comics.

• **Dan Wheeler** for initiating & implementing this project, and for the great blog and other documentations

• All zxcvbn open-source **contributors**

• **Gal Zellermayer** for KISS’ing the slides with bunch of tips.

• **Keren Shlomi** for design consulting, moral support and endless inspiration

• And **me : )** please let me know if you have any questions, comments, concerns, or you just want to say “hi”
All the icons for the slide were taken from the great [http://www.flaticon.com/](http://www.flaticon.com/) site, where you can find tons of beautiful icons like the ones I used on my slides.

- **Match** - [www.flaticon.com](http://www.flaticon.com/)
- **Star** - [www.flaticon.com](http://www.flaticon.com/)
- **People** - [www.flaticon.com](http://www.flaticon.com/)
- **Score** - [www.flaticon.com](http://www.flaticon.com/)
- **Search** - [http://www.flaticon.com/authors/simpleicon](http://www.flaticon.com/authors/simpleicon)
- **Timer** - [http://www.flaticon.com/authors/madebyoliver](http://www.flaticon.com/authors/madebyoliver)
- **Weight** - [http://www.flaticon.com/authors/cursor-creative](http://www.flaticon.com/authors/cursor-creative)
- **Code** - [http://www.flaticon.com/authors/dave-gandy](http://www.flaticon.com/authors/dave-gandy)
- **Think** - [http://www.flaticon.com/authors/pixel-perfect](http://www.flaticon.com/authors/pixel-perfect)
- **Spy** - [http://www.flaticon.com/authors/vectors-market](http://www.flaticon.com/authors/vectors-market)
- **Yes** - [http://www.flaticon.com/authors/dave-gandy](http://www.flaticon.com/authors/dave-gandy)
- **No** - [http://www.flaticon.com/authors/dave-gandy](http://www.flaticon.com/authors/dave-gandy)
- **Trophy** - [http://www.flaticon.com/authors/alfredo-hernandez](http://www.flaticon.com/authors/alfredo-hernandez)
- **Dict** - [http://www.freepik.com](http://www.freepik.com)
- **Reverse** - [http://www.flaticon.com/authors/creaticca-creative-agency](http://www.flaticon.com/authors/creaticca-creative-agency)
- **Sequence** - [http://www.freepik.com](http://www.freepik.com)
- **Keyboard** - [http://www.flaticon.com/authors/prosymbols](http://www.flaticon.com/authors/prosymbols)
- **Spatial** - [http://www.flaticon.com/authors/chris-veigt](http://www.flaticon.com/authors/chris-veigt)
- **Code** - [http://www.freepik.com](http://www.freepik.com)
- **Number** - [http://www.flaticon.com/authors/dave-gandy](http://www.flaticon.com/authors/dave-gandy)
- **Punctuation** - [http://www.freepik.com](http://www.freepik.com)
- **Warning** - [www.flaticon.com/authors/madebyoliver](http://www.flaticon.com/authors/madebyoliver)
- **Arrow signs** - [http://www.freepik.com](http://www.freepik.com)
- **Sign** - [http://www.flaticon.com/authors/madebyoliver](http://www.flaticon.com/authors/madebyoliver)
- **Gears** - [http://www.flaticon.com/authors/pixel-buddha](http://www.flaticon.com/authors/pixel-buddha)
- **Sand** - [http://www.flaticon.com/authors/madebyoliver](http://www.flaticon.com/authors/madebyoliver)
- **Feedback** - [http://www.flaticon.com/authors/daniel-bruce](http://www.flaticon.com/authors/daniel-bruce)
- **Count** - [http://www.freepik.com](http://www.freepik.com)
- **Sequence** - [http://www.freepik.com](http://www.freepik.com)
- **Meter** - [http://www.freepik.com](http://www.freepik.com)
- **Login title** - [http://www.freepik.com](http://www.freepik.com)
- **Lips** - [http://www.freepik.com](http://www.freepik.com)
- **File** - [http://www.flaticon.com/authors/madebyoliver](http://www.flaticon.com/authors/madebyoliver)
- **Settings** - [http://www.flaticon.com/authors/retinaicons](http://www.flaticon.com/authors/retinaicons)
- **Heart** - [http://www.flaticon.com/authors/creaticca-creative-agency](http://www.flaticon.com/authors/creaticca-creative-agency)
- **Question mark** - [http://www.flaticon.com/authors/madebyoliver](http://www.flaticon.com/authors/madebyoliver)
- **Warning** - [http://www.freepik.com](http://www.freepik.com)
- **Bubble** - [http://www.flaticon.com/authors/dave-gandy](http://www.flaticon.com/authors/dave-gandy)
- **Hi** - [http://www.freepik.com](http://www.freepik.com)
- **Password** - [http://www.freepik.com](http://www.freepik.com)
- **Checkbox** - [http://www.flaticon.com/authors/google](http://www.flaticon.com/authors/google)
- **Class** - [www.freepik.com](http://www.freepik.com)