

FANTASTIC PASSWORDS AND WHERE TO FIND THEM

PHIL NASH

 @philnash

 @phil_nash

 <https://philna.sh>

 philnash@twilio.com



MY FIRST PASSWORD:

“nash”

“atom”

I GOT HACKED

PASSWORDS ARE
TERRIBLE

GUIDELINES

GUIDELINES

- Uppercase
- Lowercase
- Numbers
- Special characters

password

Password1!

GUIDELINES

Change passwords regularly

Password123!

PATTERNS

Password1!

ULLLLLLLDS

AN EXAMPLE

WESTERN AUSTRALIA GOVERNMENT SECURITY AUDIT

234,000 passwords were assessed

1/4 of passwords were deemed "weak" passwords

1,464 passwords were "Password123"

([source](#))

WESTERN AUSTRALIA GOVERNMENT SECURITY AUDIT

No.	Password used	Accounts
1	Password123	1,464
2	Project10	994
3	support	866
4	password1	813
5	October2017	226
6	Monday01	225
7	Spring17	198
8	Sunday01	188
9	password	184
10	abcd1234	176

No.	Password used	Accounts
11	Spring2017	155
12	password2	142
13	August2017	141
14	sunday1	132
15	Welcome1	132
16	Password01	118
17	Summer01	102
18	Logitech1	98
19	support1	96
20	Summer17	96

Source: OAG

MY "BEST" PASSWORD

- 8 characters long
- Numbers and letters (uppercase only)
- Model number of my hi-fi

I GOT HACKED

REPETITION



last.fm



BREACHES

DISQUS

bitly

tumblr.

The image shows a browser window with the URL <https://haveibeenpwned.com>. The page features a dark blue header with navigation links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area has a large white rounded rectangle containing the text `';--have i been pwned?`. Below this is a subtitle: "Check if you have an account that has been compromised in a data breach". A search bar with the placeholder "email address" and a "pwned?" button is positioned below the subtitle. A promotional banner for 1Password is visible, with the text "Generate secure, unique passwords for every account" and a link to "Learn more at 1Password.com". The footer displays four statistics: 313 pwned websites, 5,429,399,504 pwned accounts, 79,576 pastes, and 86,888,010 paste accounts.

Have I Been Pwned: Check if you have an account that has been compromised in a data breach

email address pwned?

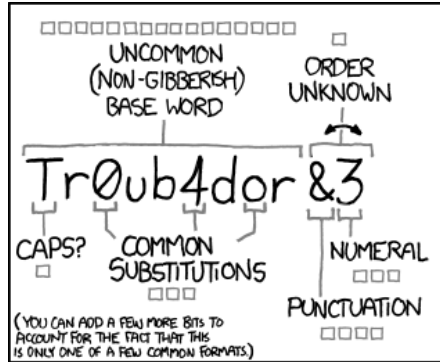
Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

313	5,429,399,504	79,576	86,888,010
pwned websites	pwned accounts	pastes	paste accounts

HOW DO WE FIX
THIS?

THE GUIDELINES
WERE WRONG



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

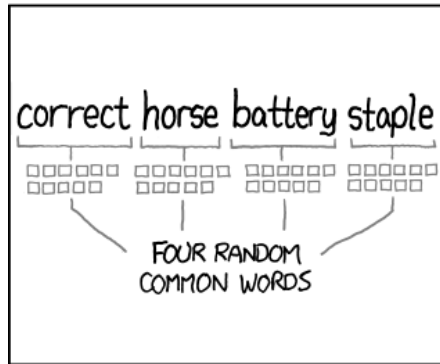
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

NEW GUIDELINES

From the ACSC, the NCSC and NIST

- At least 13 characters
- Accept all characters
- Don't allow insecure passwords
 - Dictionary words
 - Repeated or sequential characters (e.g. 'aaaaaa', '1234abcd')
 - Context specific words (e.g. username, email, app name)
 - Passwords that have been in a breach

IN RUBY?

DEVISE

```
config.password_length = 6..128
```

AUTHLOGIC

```
01. validates :password,  
02.   confirmation: { if: require_password? },  
03.   length: {  
04.     minimum: 8,  
05.     if: require_password?  
06.   }
```

CLEARANCE

Nothing

SUGGESTIONS

```
validates :password, length: { minimum: 14 }
```

nospw

strong_password

zxcvbn

NOBSPW

```
01. pwc = NOBSPW::PasswordChecker.new password: 'philnashrules',  
02.   name: 'Phil Nash',  
03.   username: 'philnash',  
04.   email: 'philnash@twilio.com'  
05. pwc.strong?  
06. pwc.weak?  
07. pwc.weak_password_reasons
```


ZXCVBN

```
01. test = Zxcvbn.test("philnashrules", ["philnash"])
```

```
02. test.score
```

```
03. test.feedback.suggestions
```

DEMO

INSECURE PASSWORDS?

PWNED PASSWORDS

PWNED PASSWORDS

572,611,621 passwords previously exposed in data breaches

PWNED PASSWORDS API

⚠ Don't worry ⚠

PWNED PASSWORDS API

1. Get the SHA1 hash of the password
2. Take the first 5 characters of the hash
3. `https://api.pwnedpasswords.com/range/#{prefix}`
4. Check if the remainder of the hash is in the result

PWNED GEM

DEMO

PWNED

<https://github.com/philnash/pwned>

[devise-pwned_password](#)

NEXT LEVEL

TWO FACTOR AUTHENTICATION

PASSWORDS ARE
TERRIBLE

PASSWORD
GUIDELINES ARE
WORSE

MAKE
PASSWORDS
LONGER

CHECK AGAINST
BREACHES

AND

DICTIONARIES

IMPLEMENT TWO FACTOR AUTHENTICATION

THANKS!

 @philnash

 @phil_nash

 <https://philna.sh>

 philnash@twilio.com





Tom Carr

@ItsMeTomC



"Your password must contain at least 8 letters, a capital, a plot, a protagonist with good character development, a twist & a happy ending."

11:56 PM · Oct 13, 2014



3.3K



4.7K people are Tweeting about this