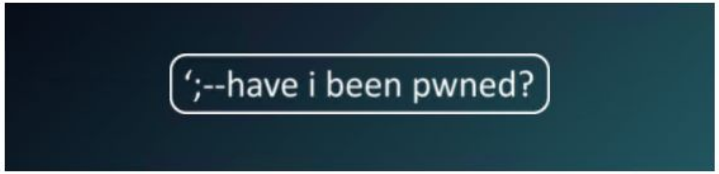
Releasing the Cracken

A Data Driven Approach for Password Generation

Shmuel Amar & Or Safran

You're one of [redacted] people pwned in the [redacted]

Have I Been Pwned <noreply@haveibeenpwned.com>
to [redacted]



You've been pwned!

You signed up for notifications when your account was pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

Email found:	[redacted]
Breach:	
Date of breach:	
Number of accounts:	
Compromised data:	
Description:	

RockYou2021: largest password compilation of all time leaked online with 8.4 billion entries

The 773 Million Record "Collection #1" Data Breach

Huge Twitch leak exposes source code, passwords - what you need to do

Every single Yahoo account was hacked - 3 billion in all

Who?

Shmuel Amar

Architect@Proofpoint

NPRE Team

NLP Lab, BIU

Or Safran

TL@Proofpoint
Research Team

Security U Data U Cloud

Agenda

- Why passwords are still exploited?
- Its hard to crack long & simple passwords
- Creating **Smartlists**
- Experiment #1: Tuning Smartlists params
- **Cracken** Demo
- Experiment #2: Cracking never revealed hashes
- Summary & Next Steps

1

Passwords? Passwords!!

Why passwords are still exploited

Which Is Better?

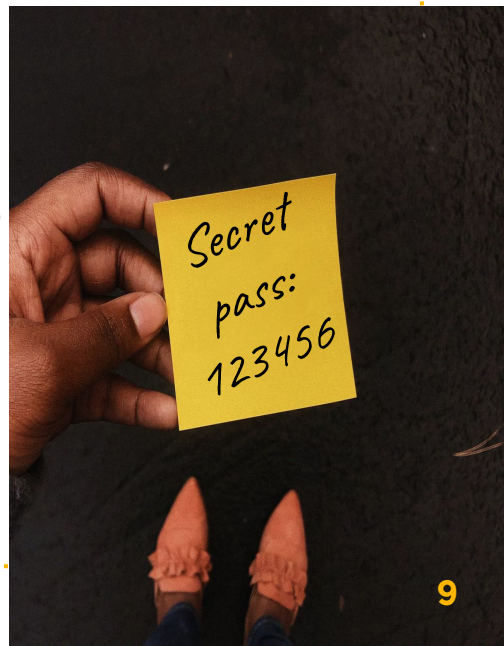
livelifelikeme08

VS

fqW34mF87u

Passwords are Obsolete?

- MFA - Bypassed
- OAuth - Applications
- Yubikey - Not Used
- Password Managers - Misused
- Leak to attack takes minutes



Why?

- Password reuse
- Survey by google claim 65% users reuse passwords

Remember: Recycle everything you can, but **do not** recycle your passwords.

Why?

October 11, 2021 By Pierluigi Paganini

DEV-0343: Iran-linked threat actors are targeting US and Israeli defense technology companies leveraging password spraying attacks.

MFA (Multi-Factor Authentication)

- 2 out of 3 factors:
  - knowledge (something the user and only the user knows)
  - possession (something the user and only the user has)
  - inherence (something the user and only the user is)
- Can be implemented with SMS, Authenticator, etc.
- Microsoft claims that MFA blocks over 99.9% account compromise attacks

MFA != SilverBullet

- Multi-factor authentication (MFA) bypass
  - Real Time Phishing
  - Channel Jacking
  - Legacy Protocols
  - Vulnerability

Real-time phishing

- Man-in-the-Middle (MITM) type of attack
  - Proxy between target and victim
- Interactive phishing
- Hard to automate
- Requires manual work
- Need to be online with the target

Channel-jacking

- MITB (Man-In-The-Browser) Malware
- Rogue Cell Tower
- Phone number takeover
- Hacking to the voice answering machine

TrickBot Pushing a 2FA Bypass App to Bank Customers in Germany

March 24, 2020 | By Pavel Asinovsky | 13 min read

Legacy Protocols

"out with the new in with the old"

- POP, IMAP, SMTP, MAPI

Vulnerability Vector

- Research once, use many (times)
- Can be very simple to activate and integrate
- Can be hard to detect, sometimes even impossible

New vulnerabilities allow hackers to bypass MFA for Microsoft 365

By Anthony Spadafora (Pro) September 17, 2020

Attacks

User Enumeration

Password Spraying

Brute Force

User Enumeration

Random User working for **Organization.fake**

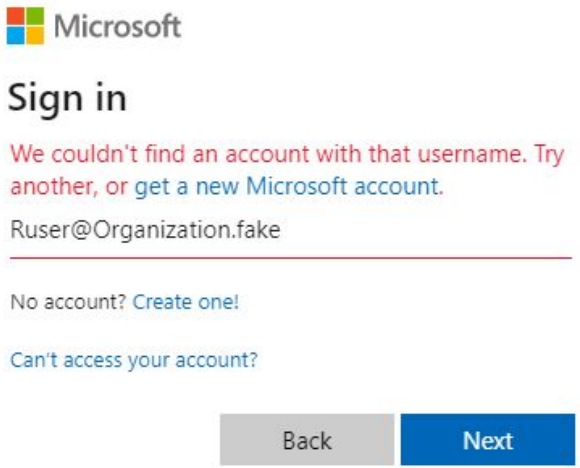
Ruser@Organization.fake

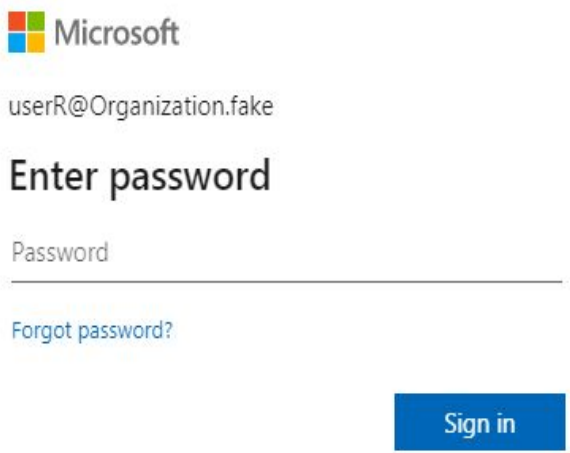
userR@Organization.fake

Random.User@Organization.fake

...

User Enumeration





Attacks

User Enumeration

Password Spraying

Brute Force

Password Spraying

userA@Organization.fake, **userB**@Organization.fake,
userC@Organization.fake, **userD**@Organization.fake...

Password: LetMeIn!

Brute Force

User Enumeration

Password Spraying

Brute Force

o365spray

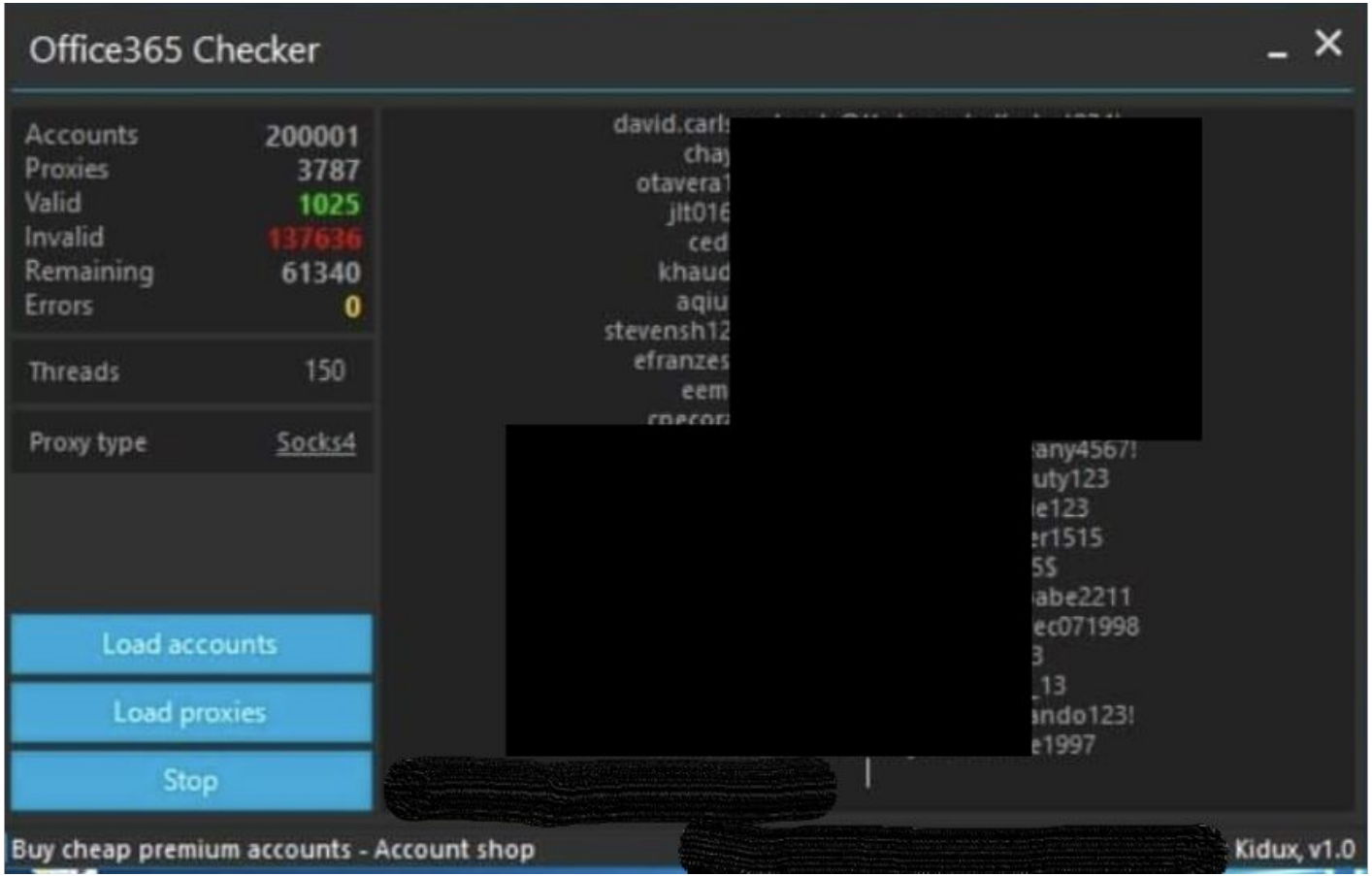
> For educational, authorized and/or research purposes only.

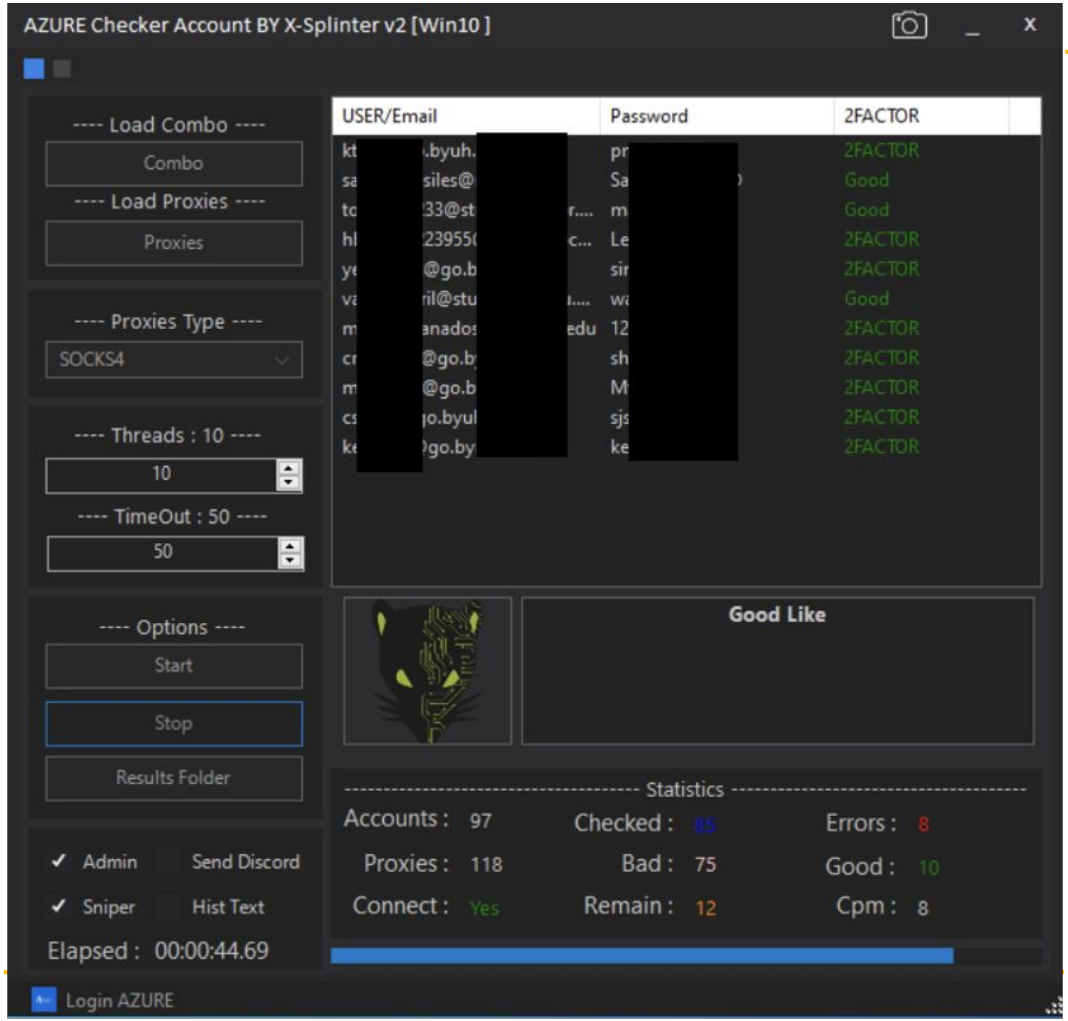
o365spray a username enumeration and password spraying tool aimed at Microsoft Office 365 (O365). This tool reimplements a collection of enumeration and spray techniques researched and identified by those mentioned in

Omnispray

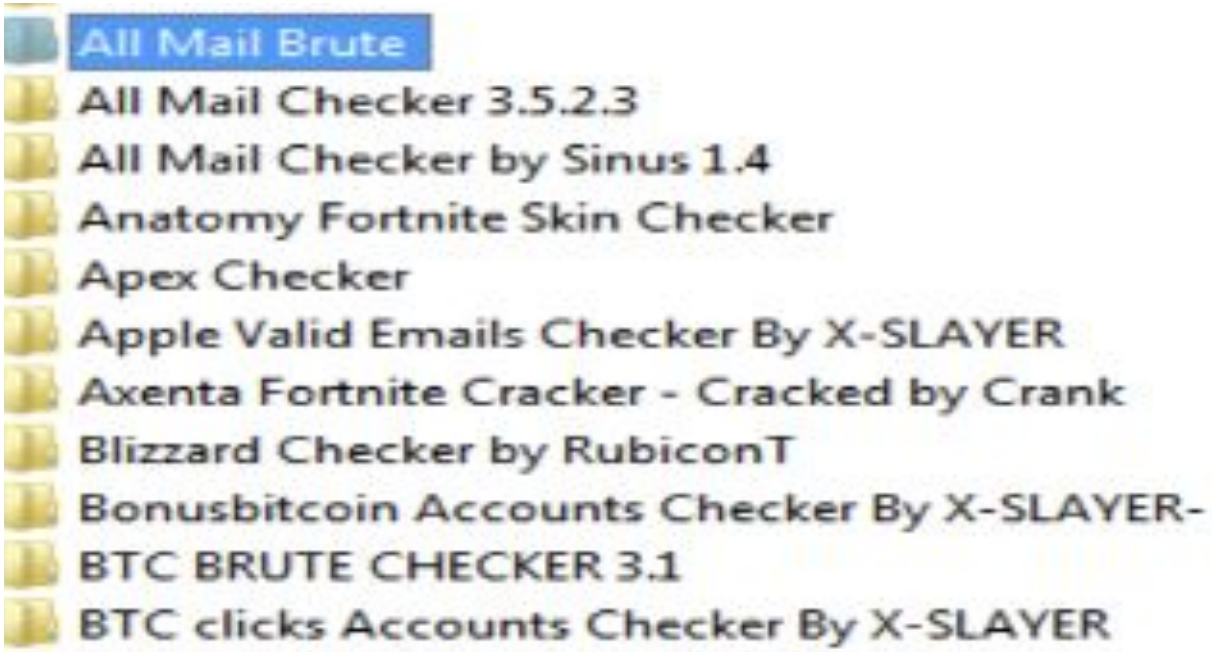
> Omnispray | Modular Enumeration and Password Spraying Framework -- v0.1.4

Omnispray aims to replace tools such as o365spray and provide a modular framework to expand enumeration and spraying beyond just a single target/application.


Office365 Checker
Accounts 200001
Proxies 3787
Valid 1025
Invalid 137636
Remaining 61340
Errors 0
Threads 150
Proxy type Socks4
Load accounts
Load proxies
Stop
Buy cheap premium accounts - Account shop
Kidux, v1.0


AZURE Checker Account BY X-Splinter v2 [Win10]
---- Load Combo ----
Combo
---- Load Proxies ----
Proxies
---- Proxies Type ----
SOCKS4
---- Threads : 10 ----
10
---- TimeOut : 50 ----
50
---- Options ----
Start
Stop
Results Folder
Admin
Send Discord
Sniper
Hist Text
Elapsed : 00:00:44.69
USER/Email
Password
2FACTOR
2FACTOR
Good
Good
2FACTOR
2FACTOR
Good
2FACTOR
2FACTOR
2FACTOR
2FACTOR
2FACTOR
Good Like
Statistics
Accounts : 97
Checked : 85
Errors : 8
Proxies : 118
Bad : 75
Good : 10
Connect : Yes
Remain : 12
Cpm : 8
Login AZURE

All Mail Brute	8 734 766	3 259 639	2021-06-12 15:09
All Mail Checker 3.5.2.3	7 555 114	2 752 260	2021-06-12 15:09
All Mail Checker by Sinus 1.4	9 064 261	3 334 556	2021-06-12 15:09
Anatomy Fortnite Skin Checker	5 232 277	2 187 718	2021-06-12 15:09
Apex Checker	36 963 141	35 491 998	2021-06-12 15:09
Apple Valid Emails Checker By X-SLAYER	4 011 845	1 918 236	2021-06-12 15:09
Axenta Fortnite Cracker - Cracked by Crank	13 346 687	5 914 653	2021-06-12 15:09
Blizzard Checker by RubiconT	16 182 085	4 806 132	2021-06-12 15:09
Bonusbitcoin Accounts Checker By X-SLAYER-	3 655 604	1 619 786	2021-06-12 15:09
BTC BRUTE CHECKER 3.1	49 450 853	15 818 089	2021-06-12 15:09
BTC clicks Accounts Checker By X-SLAYER	3 585 538	1 530 193	2021-06-12 15:09
Checker N3tflix Cracked BY Scorpio	5 105 861	1 891 684	2021-06-12 15:09
Coinify Accounts Checker By X-SLAYER	3 565 381	1 518 073	2021-06-12 15:09
Crunchyroll Checker by xRisky	16 569 635	5 557 095	2021-06-12 15:09
CyberGhost VPN Checker by xRisky	3 659 679	1 875 829	2021-06-12 15:09
Death By Captcha Accounts Checker By X-SLAYER	4 687 563	2 040 256	2021-06-12 15:09
Discord Agora's Token Checker	842 108	440 589	2021-06-12 15:09
Discord Checker by xPolish	1 029 957	494 909	2021-06-12 15:09
Discord Token Checker ULTRA	8 607 748	7 475 996	2021-06-12 15:09
Disney Checker	10 985 222	8 676 949	2021-06-12 15:09
eBay BruteChecker v2	8 160 069	2 971 944	2021-06-12 15:09
ebay Checker Account By X-KILLER	3 780 933	1 616 435	2021-06-12 15:09
Ebay Register Checker	8 801 132	4 145 348	2021-06-12 15:09
EduMail-AccessChecker	26 426 664	23 820 860	2021-06-12 15:09
Email Access Checker _atr3	5 873 385	2 225 743	2021-06-12 15:09
F.PSN Checker By Angeal v1.1.0	4 592 515	1 276 922	2021-06-12 15:09
Facebook Accounts Checker By X-SLAYER	10 648 705	4 716 351	2021-06-12 15:09
Facebook Checkers	21 824 519	5 707 050	2021-06-12 15:09
Fortlegends Checker [Crack.sx]	8 032 588	3 373 767	2021-06-12 15:09
Fortnite Checker F.A.K	31 266 880	8 820 754	2021-06-12 15:09
Fortnite Checker Keker 1_0_0_79	4 236 231	1 870 524	2021-06-12 15:09
Fortnite Checker OtimCLR3_	3 941 388	1 849 511	2021-06-12 15:09
Fortnite Skinner Checker V1.9.1	2 697 798	1 336 512	2021-06-12 15:09
freebitco.in Checker Account By X-KILLER	3 558 213	1 595 108	2021-06-12 15:09
Godaddy Checker Cracked	3 411 988	1 189 092	2021-06-12 15:09
Godaddy.com REG CHECKER BY ZARAMSIM Fixed By x-slayer.fun	2 885 189	1 778 231	2021-06-12 15:09
GoldFlix GC Netflix Checker	2 096 669	774 500	2021-06-12 15:09


All Mail Brute
All Mail Checker 3.5.2.3
All Mail Checker by Sinus 1.4
Anatomy Fortnite Skin Checker
Apex Checker
Apple Valid Emails Checker By X-SLAYER
Axenta Fortnite Cracker - Cracked by Crank
Blizzard Checker by RubiconT
Bonusbitcoin Accounts Checker By X-SLAYER-
BTC BRUTE CHECKER 3.1
BTC clicks Accounts Checker By X-SLAYER

Why - Statistics

- 59% of organizations rely on human memory to manage passwords
- 66% of Americans use the same password across multiple online accounts
- 80% of hacking-related breaches are caused by stolen and reused credentials

Why - Statistics

- An estimated 81% of data breaches are due to poor password security
- 543 million employee credentials for Fortune 1000 companies are circulating on commonly used underground hacking forums

Why - Statistics (H1 2021)

- **90% organizations attacked by either**
  - Bruteforce
  - User-enumeration
  - Password Spraying
  - Credential Stuffing
- **11% Success Rate**
- **Most Affected Industries**

Why - Statistics

- **90% organizations attacked by either**
- **11% Success Rate**
- **Most Affected Industries**
  - Education
  - Pharmaceuticals
  - Hospitality/Leisure
  - Automotive industries

2

Why We Need Smartlists?

Its hard to crack long & simple passwords

Which Is Better?

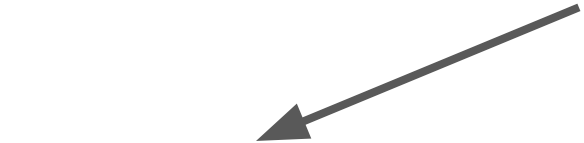
livelifelikeme08

VS

fqW34mF87u

Which Is Better?

livelifelikeme08

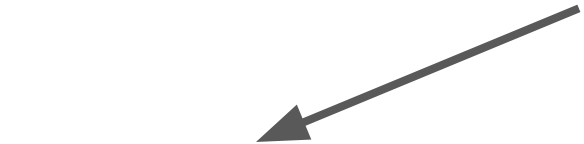


VS

fqW34mF87u

Which Is Better?

livelifelikeme08



VS

fqW34mF87u

Which Is Better?

livelifelikeme08

VS

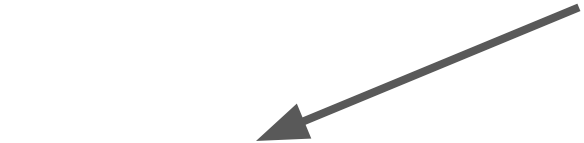
Rockyou

fqW34mF87u

Random

Which Is Better?

livelifelikeme08



VS

fqW34mF87u

- Every person on earth chooses a password of same keyspace Probability that anyone chose it is ~ 0.000001%

Which Is Better?

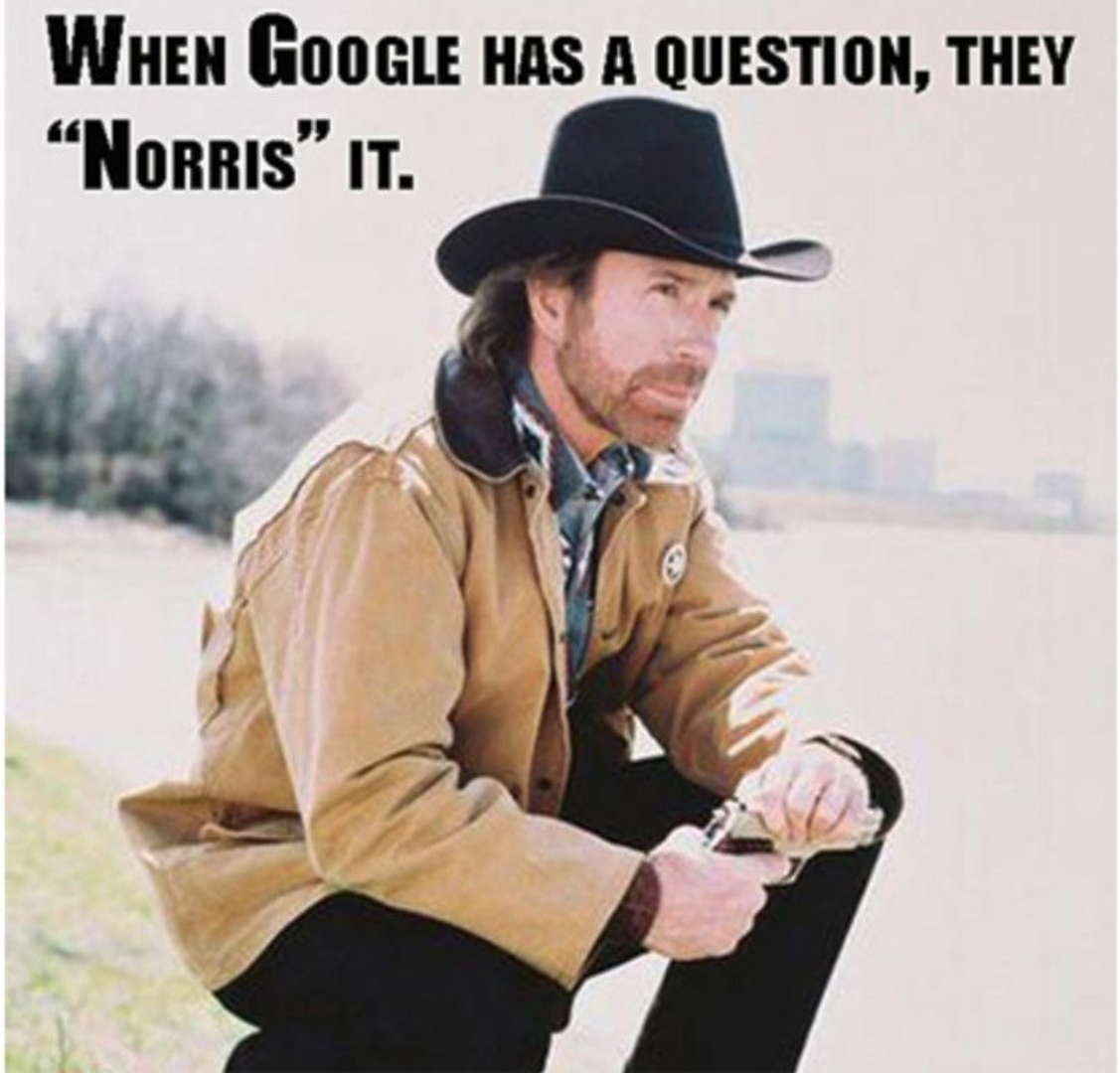
livelifelikeme08

VS

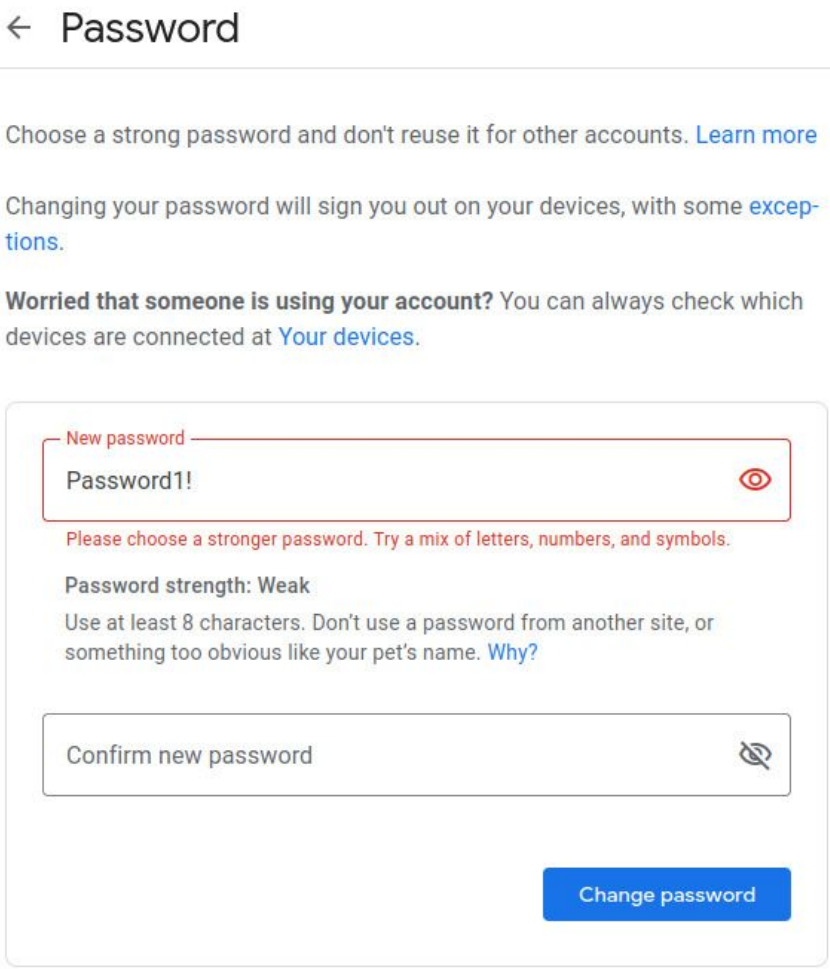
fqW34mF87u

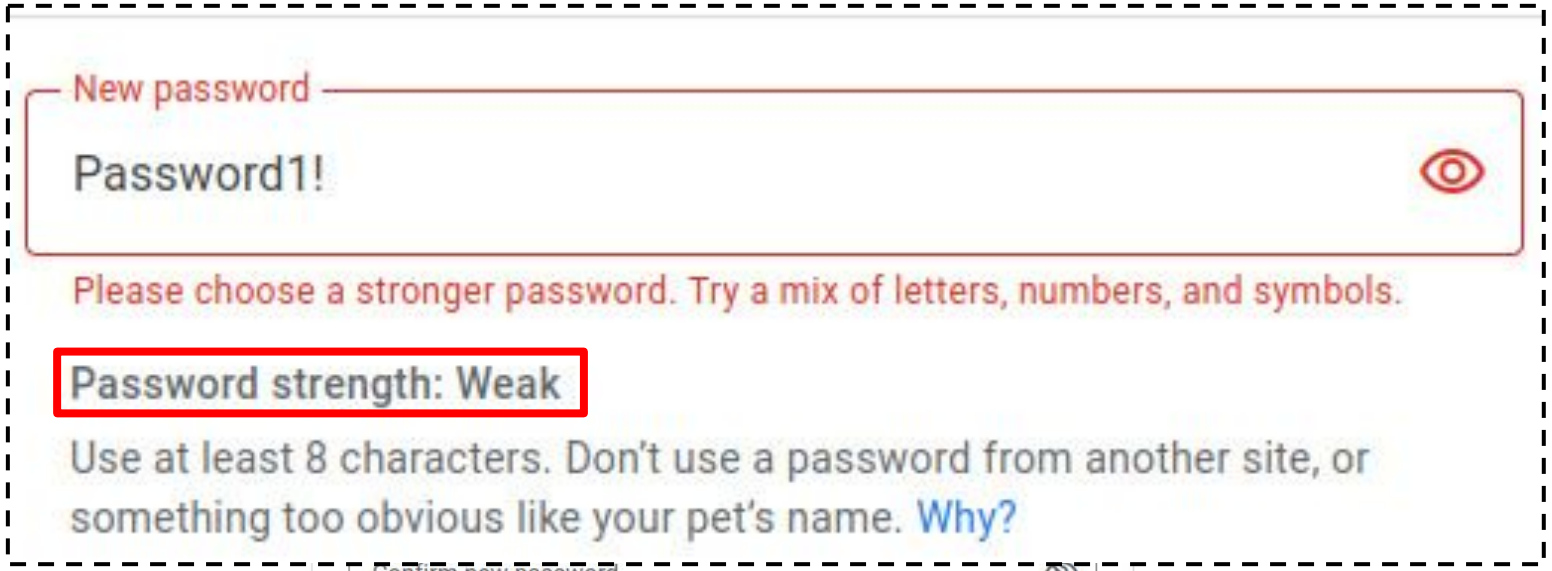
Lets estimate strengths!

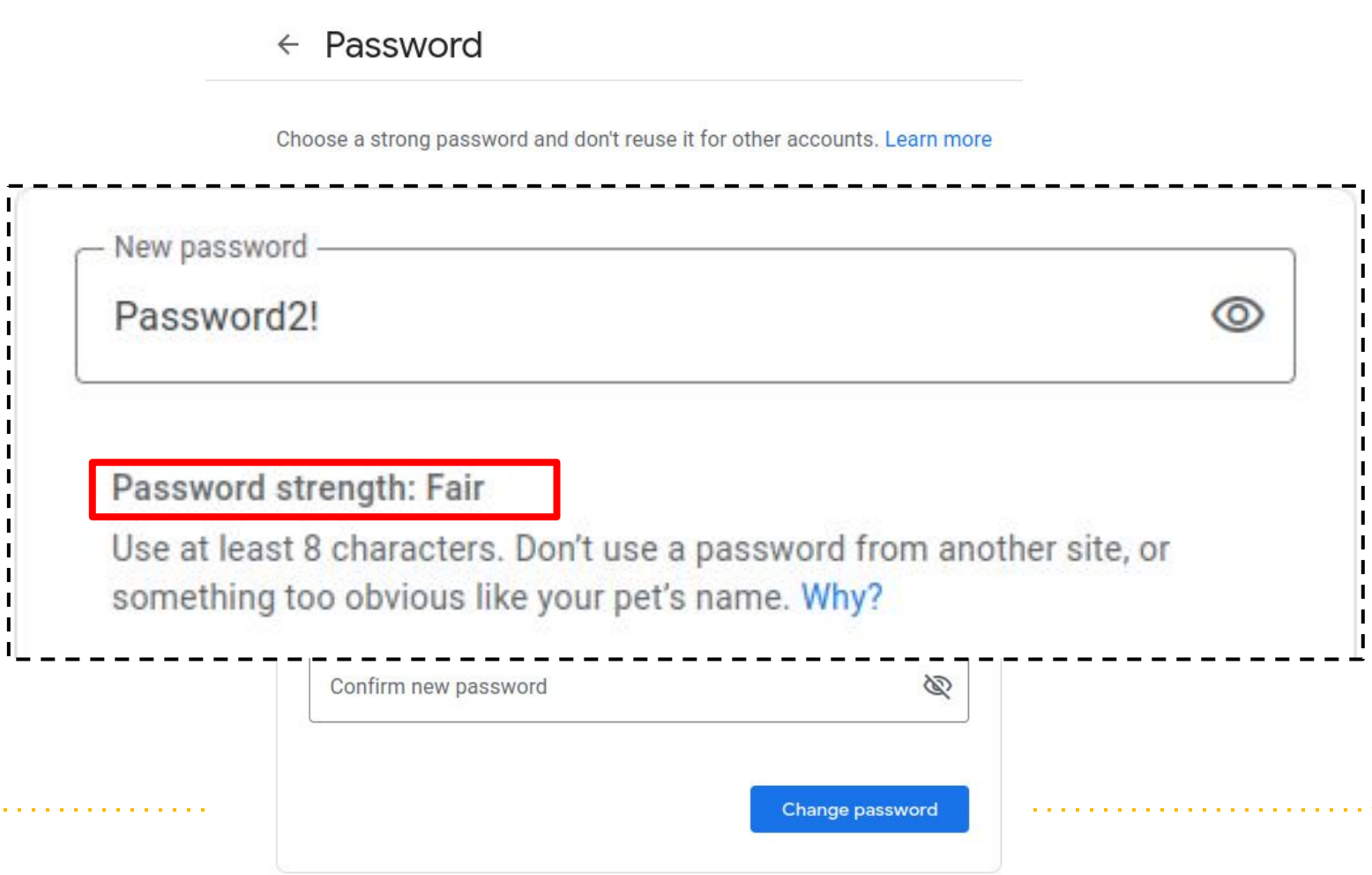

Google

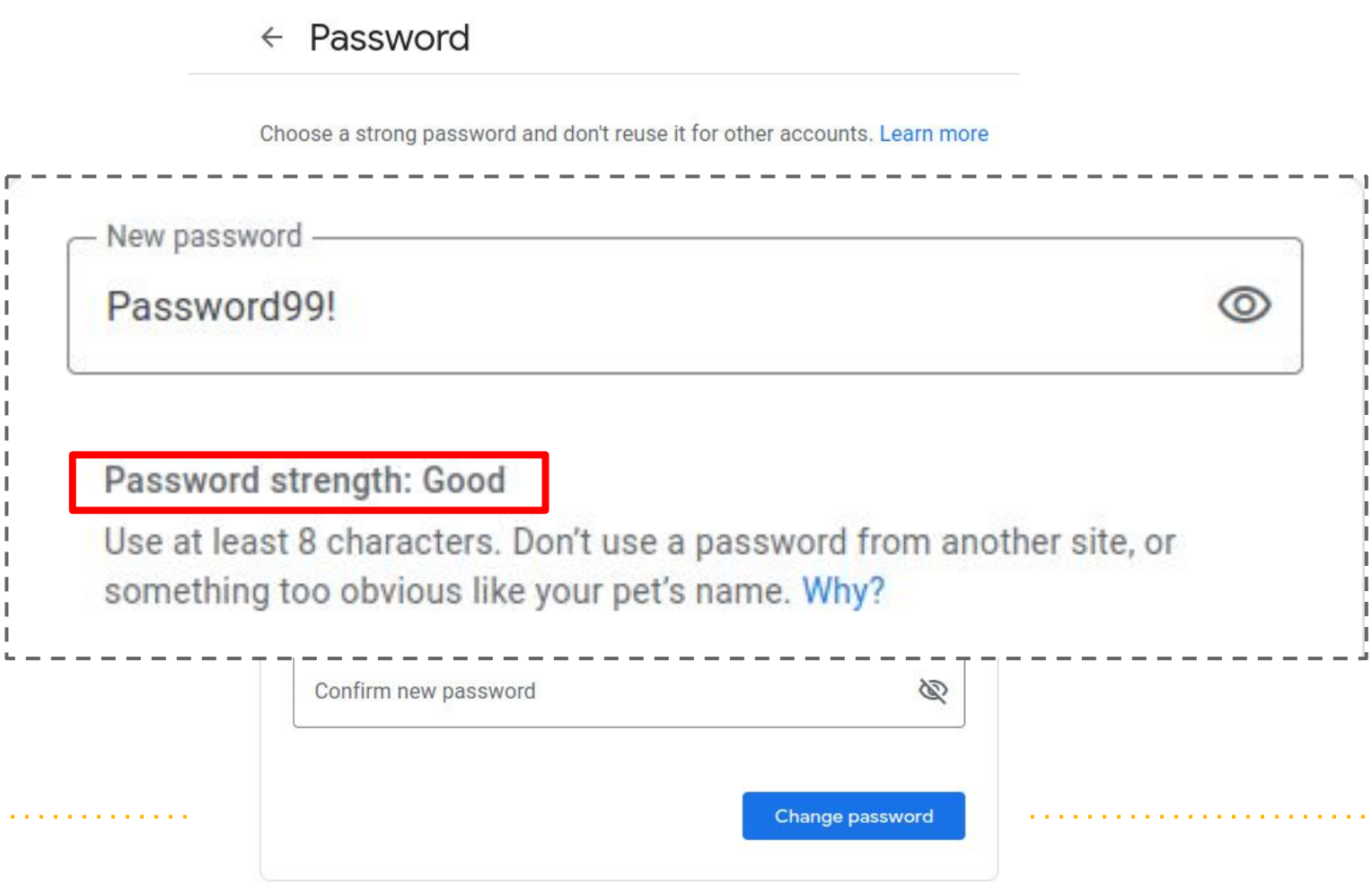

WHEN GOOGLE HAS A QUESTION, THEY
"NORRIS" IT.

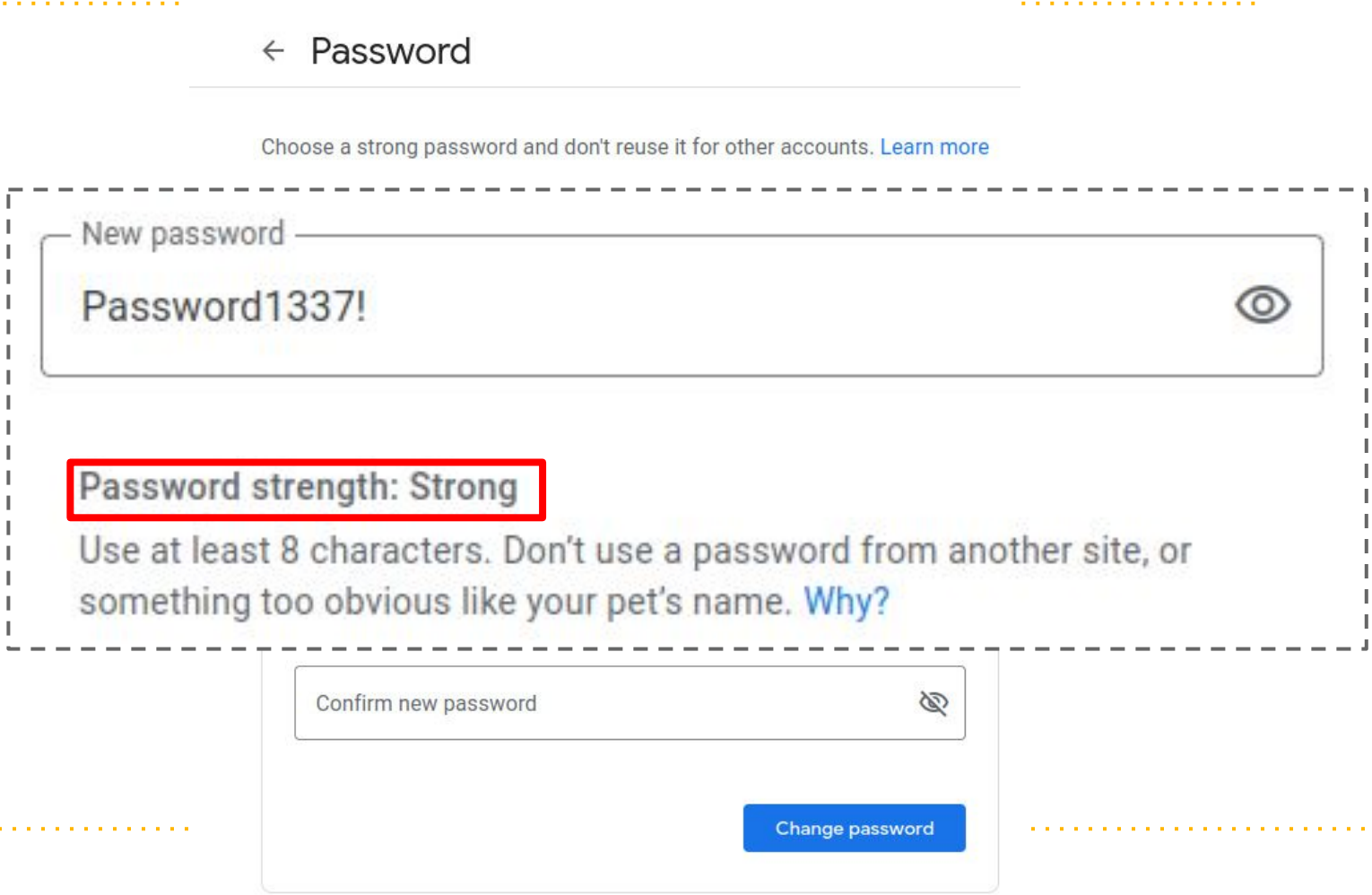

Google

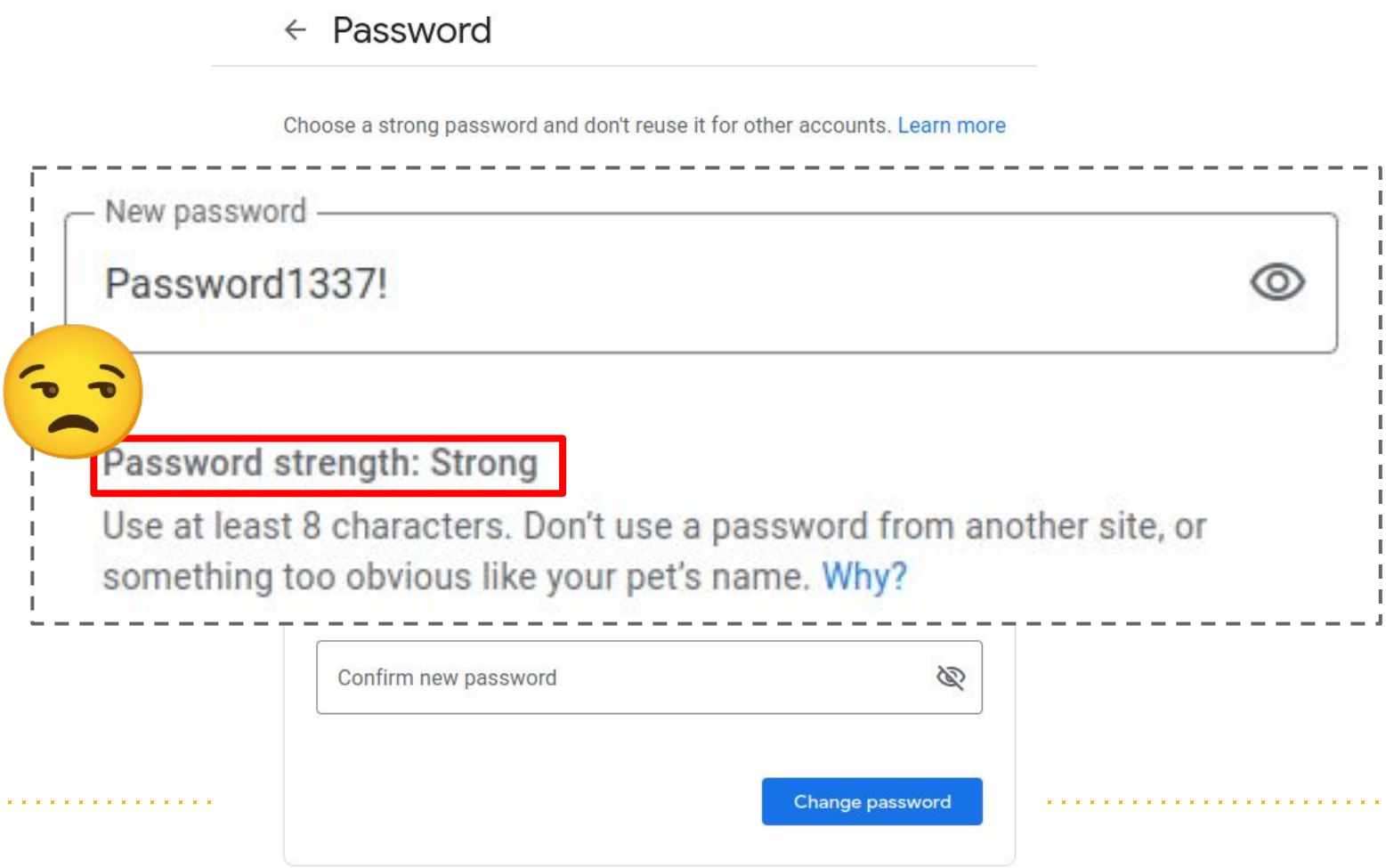

Password
Choose a strong password and don't reuse it for other accounts. Learn more
Changing your password will sign you out on your devices, with some exceptions.
Worried that someone is using your account? You can always check which devices are connected at Your devices.
New password
Password1!
Please choose a stronger password. Try a mix of letters, numbers, and symbols.
Password strength: Weak
Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?
Confirm new password
Change password


Password
Choose a strong password and don't reuse it for other accounts. Learn more
New password
Password1!
Please choose a stronger password. Try a mix of letters, numbers, and symbols.
Password strength: Weak
Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?
Confirm new password
Change password


Password
Choose a strong password and don't reuse it for other accounts. Learn more
New password
Password2!
Password strength: Fair
Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?
Confirm new password
Change password


Password
Choose a strong password and don't reuse it for other accounts. Learn more
New password
Password99!
Password strength: Good
Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?
Confirm new password
Change password


Password
Choose a strong password and don't reuse it for other accounts. Learn more
New password
Password1337!
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?
Confirm new password
Change password


Password
Choose a strong password and don't reuse it for other accounts. Learn more
New password
Password1337!
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?
Confirm new password
Change password


Google

Try #1 - Bruteforce

len(livelifelikeme08)=16

VS

len(fqW34mF87u)=10

Try #1 - Bruteforce

$$cost(livelifelikeme08) = 36^{16}$$

VS

$$cost(fqW34mF87u) = 62^{10}$$

36 = 26 lowercase + 10 digits
62 = 26 lowercase + 26 uppercase + 10 digits

Try #1 - Bruteforce

$$cost(livelifelikeme08) = 36^{16} \approx 2^{82}$$

VS

$$cost(fqW34mF87u) = 62^{10} \approx 2^{60}$$

36 = 26 lowercase + 10 digits
62 = 26 lowercase + 26 uppercase + 10 digits

Try #1 - Bruteforce

$\hat{H}$(livelifelikeme08)≈82

VS

$\hat{H}$(fqW34mF87u)≈60

$\hat{H}$ - estimated entropy

Try #1 - Bruteforce

$\hat{H}$(livelifelikeme08)≈82

VS

×4.2M

$\hat{H}$(fqW34mF87u)≈60

$\hat{H}$ - estimated entropy

Try #1 - Bruteforce

- Cracking time calculation:
  - **Summit** a super computer (#2 on wikipedia)
  - **Hardware** 27,648 NVIDIA Tesla V100 GPUs
  - **SHA1** ~17B hashes/sec per V100 GPU
- **Total - 470T** hashes/sec 🤯

Try #1 - Bruteforce

- **Total - 470T** hashes/sec
- Cracking **2^{60} - 41 mins**
- Cracking **2^{82} - 326 Years**

Try #1 - Bruteforce

- **Total - 470T** hashes/sec
- Cracking **2^{60} - 41 mins**
- Cracking **2^{82} - 326 Years**

Try #2 - Charset Mask Attack

livelifelikeme08

Try #2 - Charset Mask Attack

livelifelikeme08

?l?l?l?l?l?l?l?l?l?l?l?l?d?d

Lowercase

Digit

Try #2 - Charset Mask Attack

$$\text{cost}(\text{livelifelikeme08}) = 26^{14} \times 10^{2} \approx 2^{72}$$

Lowercase
Digit

Try #2 - Charset Mask Attack

$\hat{H}$(livelifelikeme08)≈72

VS

$\hat{H}$(fqW34mF87u)≈60

×4096

Lowercase
Digit

$\hat{H}$ - estimated entropy

Try #2 - Charset Mask Attack

$\hat{H}$(livelifelikeme08)≈72

VS

$\hat{H}$(fqW34mF87u)≈60

Lowercase
Digit

$\hat{H}$ - estimated entropy

Try #3 - Wordlists

livelifelikeme08

Try #3 - Wordlists

livelifelikeme08

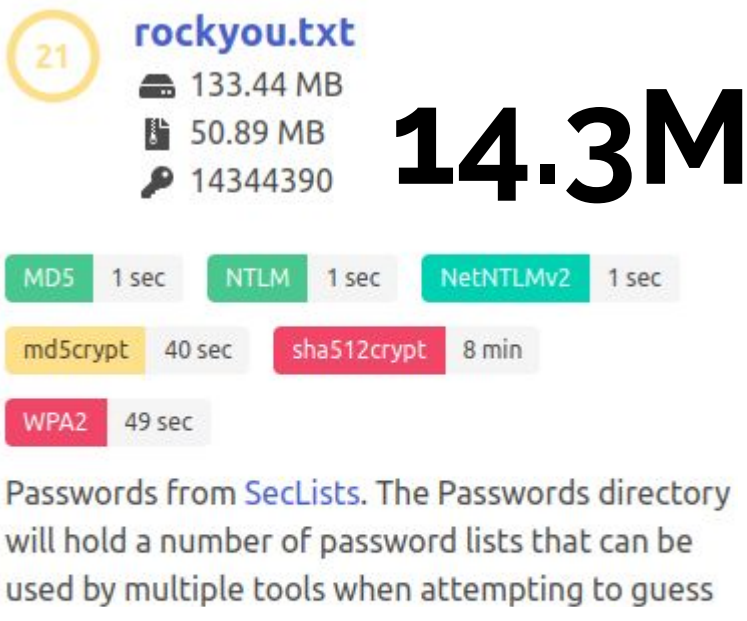
Try #3 - Wordlists

$$cost(livelifelikeme08) = |W|^5$$

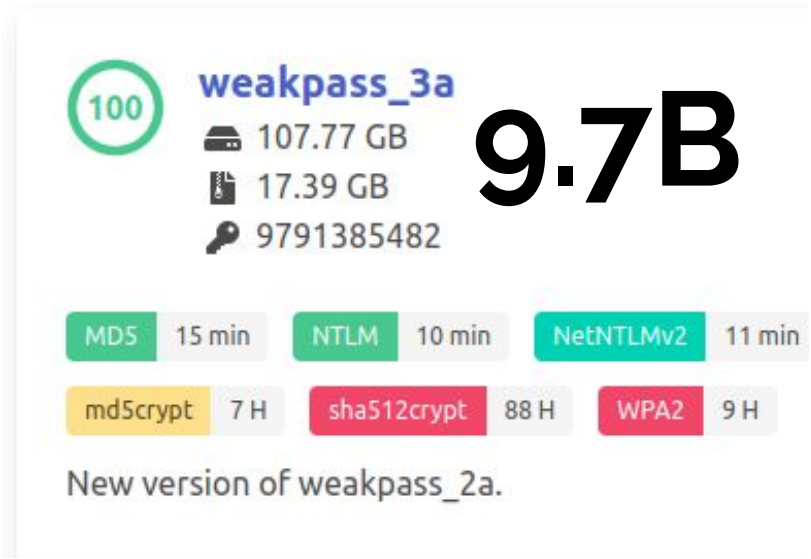
Try #3 - Wordlists

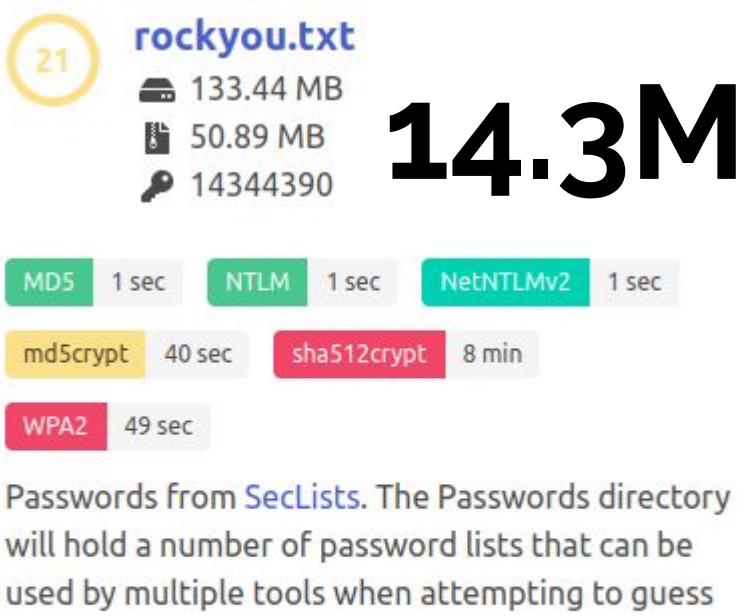
$$cost(livelifelikeme08) = |W|^5 = ??$$

Try #3 - Wordlists



https://weakpass.com

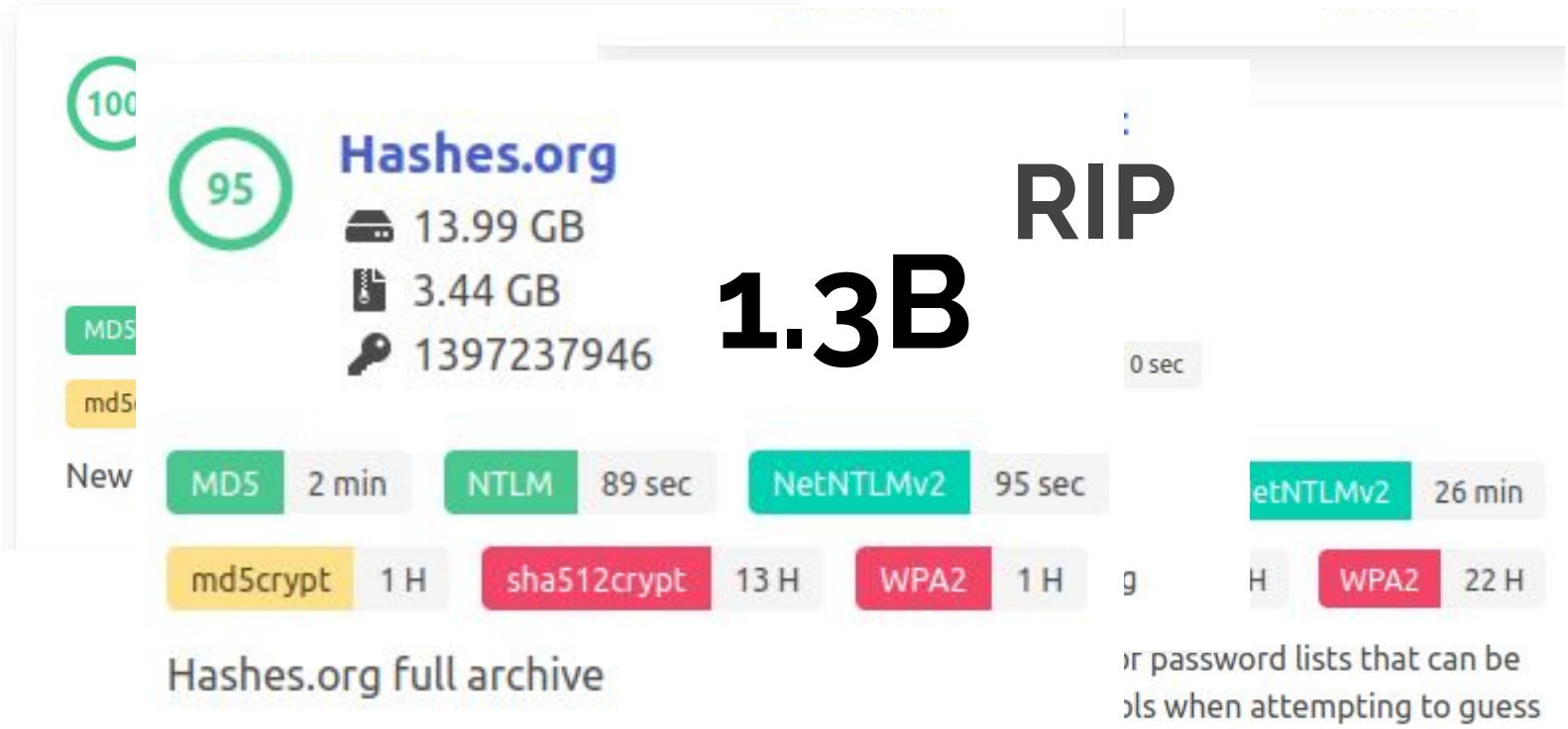




https://weakpass.com

https://weakpass.com

https://weakpass.com



https://weakpass.com

RIP

https://hashes.org

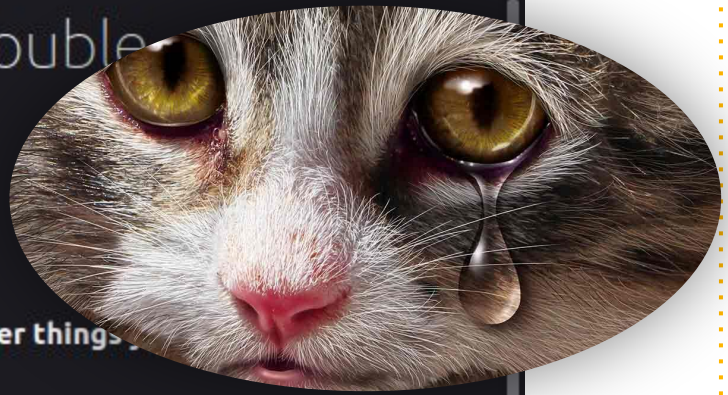
Hmm. We're having trouble finding that site.

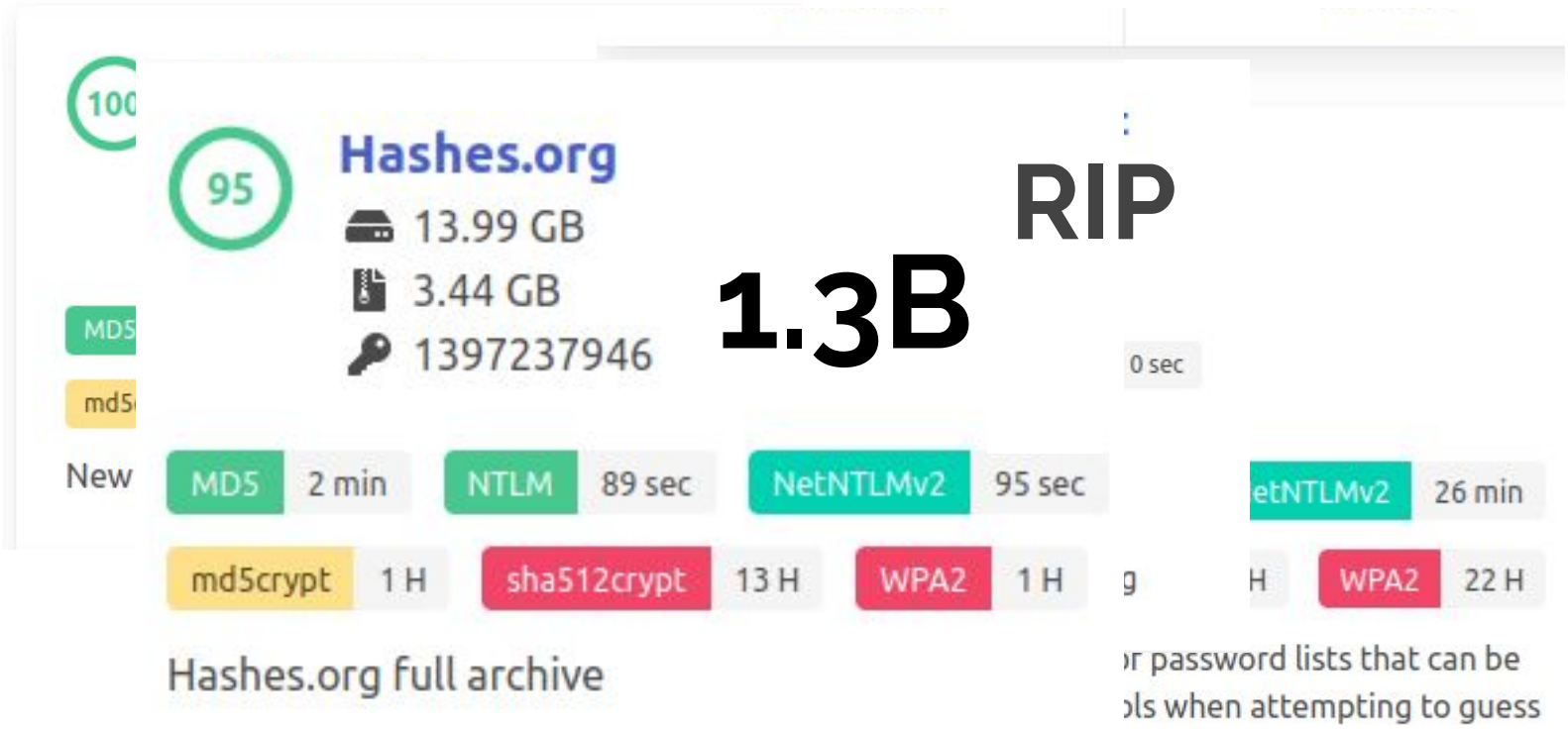
We can't connect to the server at hashes.org.

If that address is correct, here are three other things

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Try Again





https://weakpass.com

Try #3 - Wordlists

$$cost(livelifelikeme08) = |W|^5 = 14.3M^5 \approx 2^{119}$$

|W| = 14.3M - Rockyou wordlist

Try #3 - Wordlists

$cost(livelifelikeme08) = |W|^5 = 14.3M^5 \approx 2$ 🤔

|W| = 14.3M - Rockyou wordlist

Try #3 - Wordlists

$$cost(livelifelikeme08) = |W|^3 = 14.3M^3 \approx 2^{71}$$

|W| = 14.3M - Rockyou wordlist

Try #3 - Wordlists

$$cost(livelifelikeme08) = |W|^5 = 171k^5 \approx 2^{87}$$

|W| = 171k - Oxford english head words

Something in the Middle

Charsets

<=256

Single Chars

Smartlists

5k-10M

Multi Chars

Common Phrases

Wordlists

100k-10B

Full Words/Pwds

Try #3 - Wordlists

$$cost(livelifelikeme08) = |W|^5 = 171k^5 \approx 2^{87}$$

- What about:
  - Capitalization
  - Symbols
  - Numbers

Try #3 - Wordlists

$$\text{cost}(\text{livelifelikeme08}) = |W|^5 = 171k^5 \approx 2^{87}$$

|W| = 171k - Oxford english head words

Something in the Middle

Charsets

<=256

Single Chars

Wordlists

100k-10B

Full Words/Pwds

Try #4 - Smartlists

livelifelikeme08

Try #4 - Smartlists

livelifelikeme08

livelifelikeme08

Try #4 - Smartlists

5 Subwords

livelifelikeme08

livelifelikeme08

3 Subwords

Rockyou Counts

#live = 38,877

#life = 65,803

#like = 11,687

#me = 892,403

#08 = 971,690

Rockyou Counts

#livelife = 792

#likeme = 762

Try #4 - Smartlists

$$cost(livelifelikeme08) = |W|^5 = 5k^5 \approx 2^{61}$$

|W| = 5k - Small Smartlist, built from Rockyou "easy" passwords

Try #4 - Smartlists

$$cost(livelifelikeme08) = |W|^3 = 50k^3 \approx 2^{47}$$

|W| = 50k - Medium Smartlist, built from Rockyou "easy" passwords

Combining Smartlists

cost(livelikelikeme08)=

cost(?w_1?w_1?w_2?d?d)=$|W_1|^2 \times |W_2| \times 10^2 \approx 2^{47}$

$|W_1|$ = **5k** - Small Smartlist
$|W_2|$ = **50k** - Medium Smartlist

Try #4 - Smartlists

$cost(livelifelikeme08) = |W|^3 = 50k^3 \approx 2^{47}$

Feasible!!

|W| = 50k - Medium Smartlist, built from Rockyou "easy" passwords

Charset vs Hybrid Mask

livelifelikeme08

?l?l?l?l?l?l?l?l?l?l?l?l?l?l?l?d?d

?w_1?w_1?w_2?d?d

?l - Lowercase letter
?d - Digit
?w_i - Word from Wordlist i

Charset vs Hybrid Mask

livelifelikeme08

?w$_1$?w$_1$?w$_2$?d?d

?w$_1$?w$_1$?w$_1$?w$_1$?w$_1$

?w$_1$?w$_1$?d?d

?w$_1$?w$_2$?l?l?d?d

?w$_2$?w$_2$?w$_2$

Which Mask to choose?

The mask with minimal keyspace

3

Creating Smartlists

Utilizing NLP tokenizers for wordlist generation

NLP Tokenizers

- Traditional NLP models used char / word level encoding
- **BPE - Byte Pair Encoding**, a tokenization algorithm introduced on 2015
- It uses frequency of **subword** pairs to create a **compact** vocabulary of **desired size**

BPE Demo

123456

1234

1212

password

admin

BPE Demo - Init

1,2,3,4,5,6

1,2,3,4

1,2,1,2

p,a,s,s,w,o,r,d

a,d,m,i,n

BPE Demo - Init

Vocab = {1,2,3,4,5,6,p,a,s,w,o,r,d,m,i,n}

1,2,3,4,5,6

1,2,3,4

1,2,1,2

p,a,s,s,w,o,r,d

a,d,m,i,n

Find Most Common Pair

Vocab = {1,2,3,4,5,6,p,a,s,w,o,r,d,m,i,n}

1,2,3,4,5,6

1,2,3,4

1,2,**1,2**

p,a,s,s,w,o,r,d

a,d,m,i,n

#(1,2) = 4

Merge The Pair

Vocab = {1,2,3,4,5,6,p,a,s,w,o,r,d,m,i,n}

12,3,4,5,6

12,3,4

12,**12**

p,a,s,s,w,o,r,d

a,d,m,i,n

Add The Pair To The Vocab

Vocab = {1,2,3,4,5,6,p,a,s,w,o,r,d,m,i,n,**12**}

12,3,4,5,6

12,3,4

12,**12**

p,a,s,s,w,o,r,d

a,d,m,i,n

Find Most Common Pair

Vocab = {1,2,3,4,5,6,p,a,s,w,o,r,d,m,i,n,12}

12,3,4,5,6

12,3,4

12,12

p,a,s,s,w,o,r,d

a,d,m,i,n

#(12,3) = 2

Find Most Common Pair

Vocab = {1,2,3,4,5,6,p,a,s,w,o,r,d,m,i,n,12}

12,**3,4**,5,6

12,**3,4**

12,12

p,a,s,s,w,o,r,d

a,d,m,i,n

#(3,4) = 2

Find Most Common Pair

Vocab = {1,2,3,4,5,6,p,a,s,w,o,r,d,m,i,n,12}

12,3,4,5,6

12,3,4

12,12

p,a,s,s,w,o,r,d

a,d,m,i,n

#(12,3) = 2

Merge The Pair

Vocab = {1,2,3,4,5,6,p,a,s,w,o,r,d,m,i,n,12}

123,4,5,6

123,4

12,12

p,a,s,s,w,o,r,d

a,d,m,i,n

Add The Pair To The Vocab

Vocab = {1,2,3,4,5,6,p,a,s,w,o,r,d,m,i,n,12,**123**}

123,4,5,6

123,4

12,12

p,a,s,s,w,o,r,d

a,d,m,i,n

Do Until Desired Vocabulary Size Reached

Building a Smartlist

- Define desired wordlist max size (e.g. 10k)
- Choose one or more algorithms
  - BPE
  - Unigram
  - Wordpiece
- The resulting vocabulary is our **Smartlist**

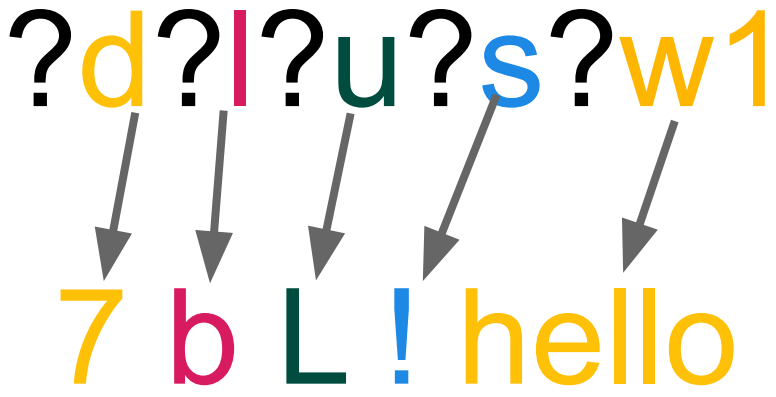
4

Smartlists Tuning

Experiment #1 - Finding good Smartlist parameters empirically

Masks

Masking Options



Many Options...

- Min String Len - [1,2,3,4]
- Max Number Size [Off,4,6]
- Tokenizers [BPE, Unigram, Wordpiece, combination]
- 5K-50M Wordlist Size

The problem

- What to choose?
- How to find what's best for a specific problem

How We Chose?

- Rockyou breach (2009) (32M)
- Tried many wordlist sizes
- Tried all algorithm combinations
- Tried Post Processing options

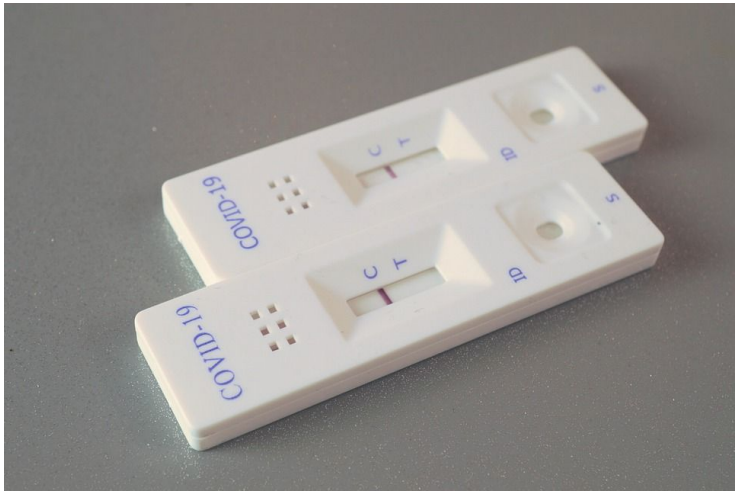
Experiment Setup

- Rockyou Passwords
- Splitted into 2 lists
  - **Easy -** to crack (charset mask keyspace < 2^{40})
  - **Hard -** to crack (charset mask keyspace > 2^{70})

Experiment Setup

- Create Smartlists with different options Using the **Easy passwords**
- Count the total **Hard passwords** found in under 2^{50} tries
- Used hybrid masking

Results



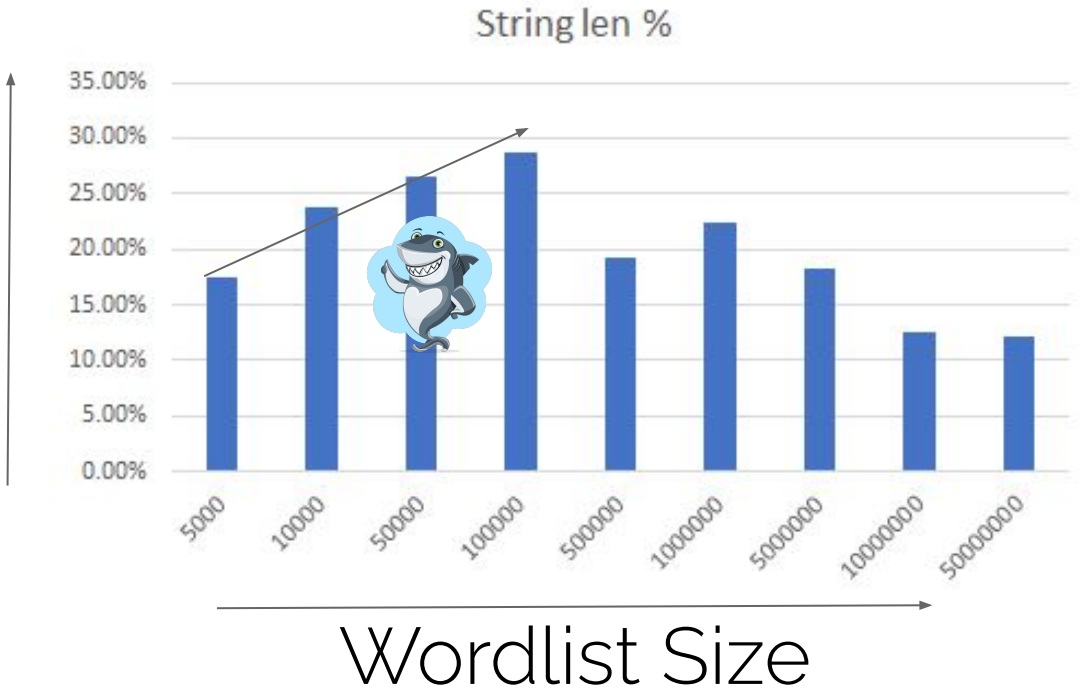
Tokenizers

% hard passwords cracked

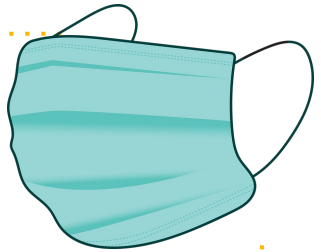
Unigram	24.18%
Bpe + Unigram	19.80%
Bpe	19.60%
Unigram + Wordpiece	19.60%
Bpe + Unigram + Wordpiece	19.20%
Bpe + Wordpiece	19.16%
Wordpiece	19.14%

Stats

Passwords cracked



Masks - Wordlists



Definitions:

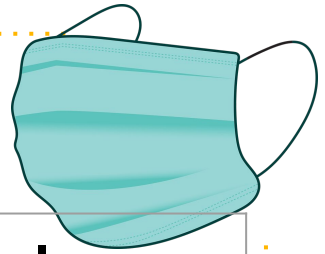
w1 - 500 most common passwords

w2 - 5k Small Smartlist

w3 - 50k Medium Smartlist

w4 - 5M Large Smartlist

Masks - Hard Passwords



Count	$\log_2$(KeySpace)	Hybrid Mask	Example
189	47.14	?w3?w3?l?w2	easyeasyxfind
109	46.38	?w3?w1?w4	easyhardquestions
93	46.17	?w4?b?b?b	questions3X!
106	46.38	?w1?w4?w3	hardquestionseasy
104	46.38	?w4?w3?w1	questionseasyhard
707	49.37	?w4?w3?w2	questionseasyfind

5

Releasing The Cracken

Cracken Demo

Cracken Commands

- **Create -** creating **Smartlists** with NLP tokenizers
- **Generate -** Fast hybrid mask (wordlists&charsets) password generator
- **Entropy -** estimating entropy and hybrid masks of passwords (analysis)

Under the Hood

- **Cracken** is written in Rust
- Cracken is **built for speed**
- ~25% faster than hashcat's MaskProcessor
  - MP claims - "*world's fastest word generator*"
- Cracken generates words **FAST** ⚡ 🦸 **:**
  - 2GB/s for Charset masks (no wordlists)
  - 1GB/s for Hybrid masks (wordlists+charsets)

Demo Time

https://github.com/shmuelamar/cracken

6

Real World Results

Experiment #2 - Cracking never revealed hashes

Xsplit Case

- Xsplit is an unsalted sha1 (2013 3M users)
- Published to the public (2015) - **OLD!**
- Rockyou hybrid masks
- Wordlist: 500, 5K, 50K, 5M
- Removed all found hashes from hashes.org
- 3 days on a **laptop** gpu (2B h/sec)

We let it run for 3 days

And it rained passwords

98% were pre-cracked

- Dealing with the hardest 2%
- Never cracked before

Over 100 cracked!

6e51edb0219067a3...:L
381e1877613f1005...:11
70a36e039b93a575...:s
62203519caa3d656...:s
232f00d6078e6ea5...:pr
5152472015e492d4...:d

Results

- Sample of masks that were useful
- Simple, long, uncracked for ~7 years

?w3?l?l?w1?d?d

profilextscreen91

leadpaexams87

?w3?d?d?w2?d?d

luck98havana99

nuts67crazy54

7

Summary

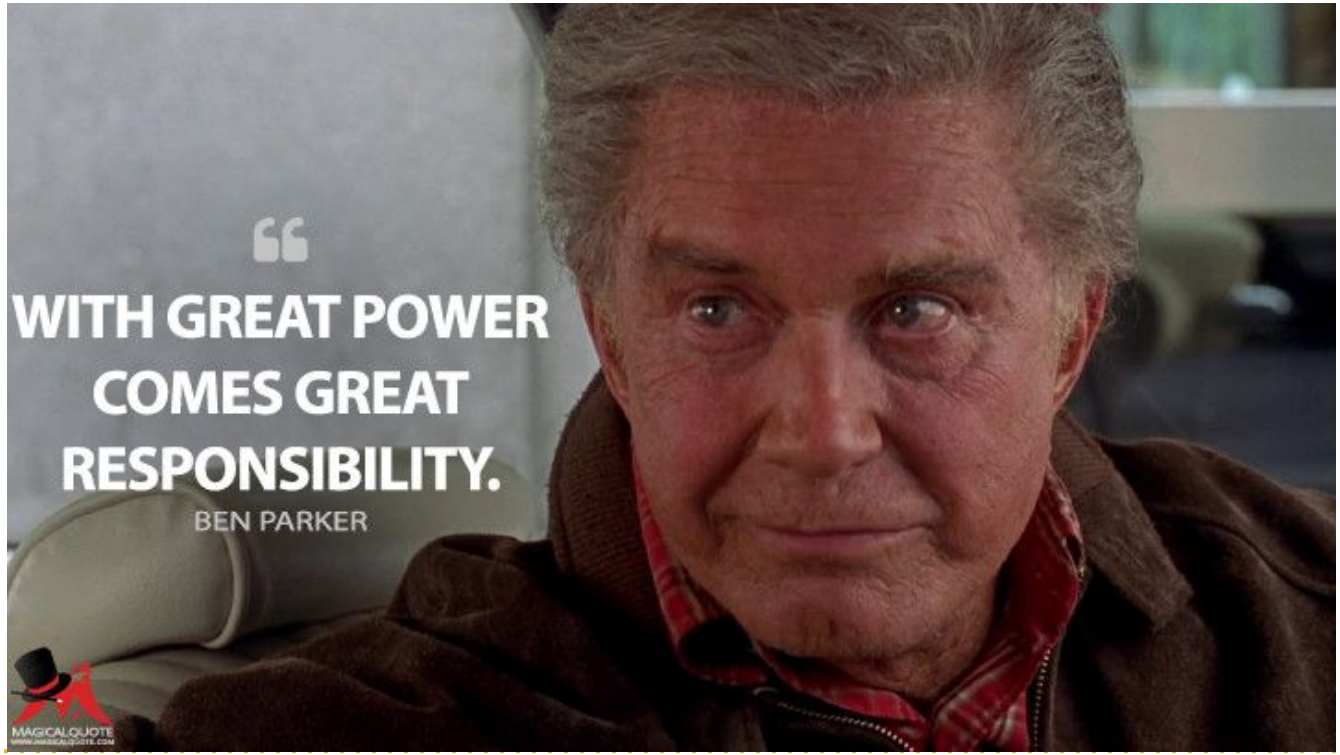
Summary

- Long but simple passwords are crackable
- Use Cracken for:
  - Creating Smartlists
  - Generating wordlists VERY Fast
  - Estimation for password strength with a new approach

What's Next? Chars -> Subwords

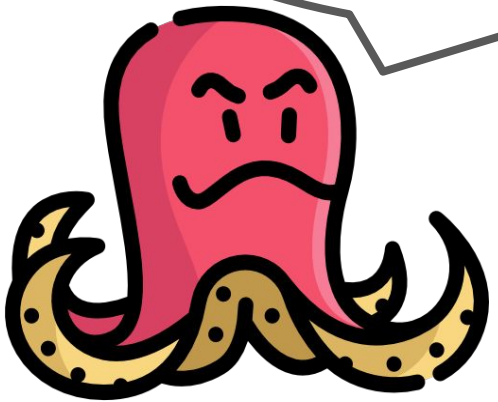
- Markov Chains:
  - p('h'|'t') -> p('world'|'hello')
- Mangling Rules (e.g. toggle case):
  - helloworld123! -> HelloWorld123!
- Replace related subwords:
  - HelloWorld123! -> HiWorld123!
  - HelloBlackhat20 -> ByeDeepsec21

And its Open Source!



Thanks!

Questions?



https://github.com/shmuelamar/cracken