

Password Hygiene

CUCUG
Quentin Barnes
July 17, 2025



Yet Another Hack, Google This Time

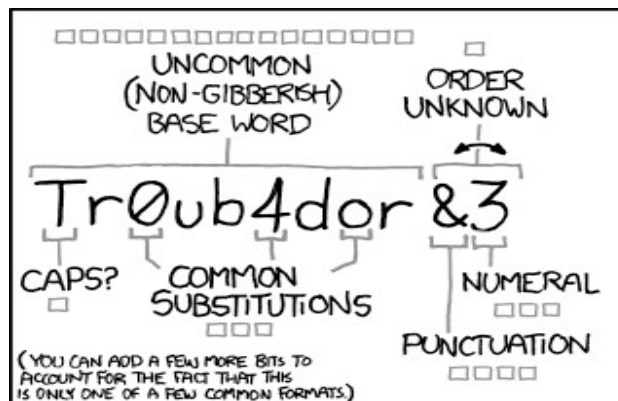
- Was reading our newsletter today
- “Gmail Warning Just Dropped-Reset Your Password ASAP” article
- Today seems like a good day to talk about “password hygiene”

Easy to Remember Passwords

- People make passwords about themselves
 - Memorable pet/friend/relative's name or location
 - Adding special date strings (MMDD) to a base password
 - Adding a sequence digit to a previous password
 - Slightly modifying password based on site's/product's name
 - Reusing passwords
- Making passwords like these are saying, "Hack ME!"

So People Use Random Passwords

- `$ pwmake 60
blcsUByriz64G`
- Now what can you do with that?
- Hard to remember, especially dozens of them!
- Write it down on post it notes?
- Typing it on a phone keyboard is annoying



~28 BITS OF ENTROPY

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

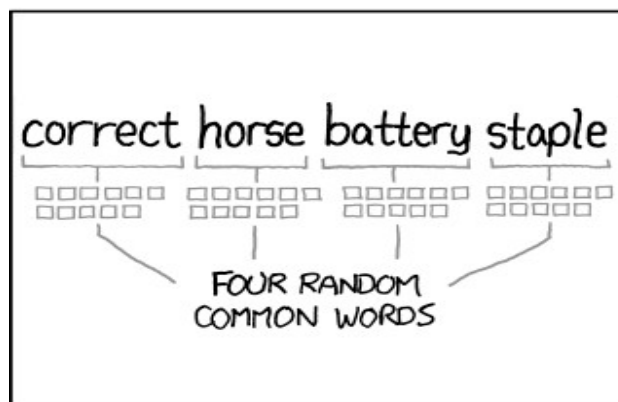
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

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.

Making Password Phrases

- Diceware word list
 - <https://theworld.com/~reinhold/dicewarewordlist.pdf>
- Real 5d6 dice
- “d20 Calculator” iOS app



Password Phrases

- Ok, so random password phrases good
- But so, so many to make them all unique
- Password managers to the rescue!
 - Only one phrase needed to unlock your PM

Common Password Managers

- 1Password
- Lastpass
- NordPass
- KeePass
- Proton Pass
- Bitwarden

Bitwarden

- Multi-platform / Cross-platform
 - Browsers, MS Windows, MacOS, Linux, iOS, Android
- Free as in beer (no cost for personal use)
- Free as in freedom (FOSS)
- Multitude of tools
 - Built-in generator for passphrases
 - Easy import / export
- Cloud and self-hosting

Demo!