

Password Security

What rules are likely to apply?

Change account password ✕

Old password:

New password:

Confirm new password:

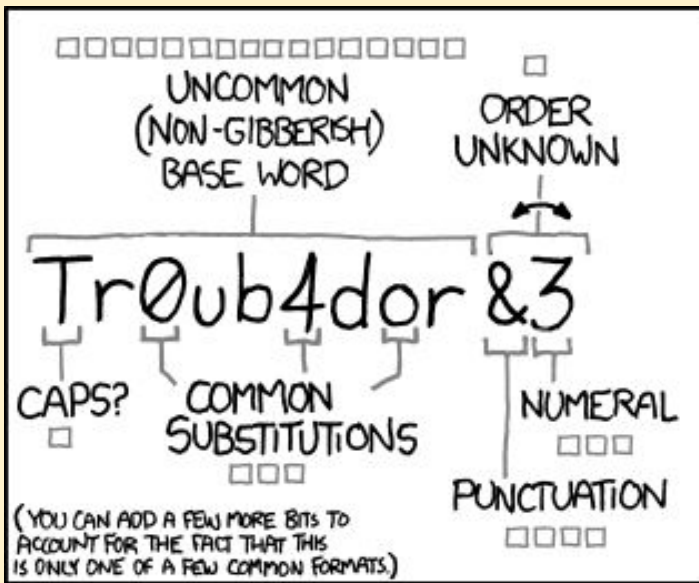
[Save](#) [Cancel](#)

Password Security

- uppercase letter?
- number?
- symbol?
- length?
- changed frequently?
- avoid common words?

Password Security

- ~~uppercase letter?~~ - usually at start
- ~~number?~~ - usually at end; 1 frequent
- symbol? - better, but watch @, 4, 3, 5 etc...
- ~~length?~~ - but 6-8 is too short
- ~~changed frequently?~~ - just add number
- avoid common words? - yes, but...



~28 BITS OF ENTROPY

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

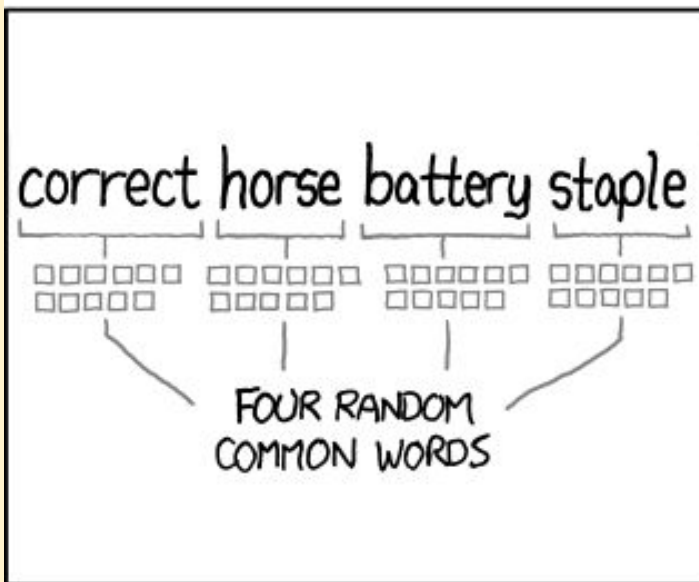
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

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.

Password Security

Given that the biggest problem is dictionaries of passwords compiled from past hacks:

- “Our focus should be on protecting passwords against **informed statistical attacks** and not brute-force attacks.”
- “When you do have to choose a password, one of the most important selection criterion should be **how many other people have also chosen that same password**”

Password Security

Password managers allow complex passwords to be set and remembered by machines and are increasingly seen as preferable to users setting their own passwords

- “Choosing a password should be something you do very infrequently”