

Password Managers 101

Everything you need to know even if you didn't want to...

Top Password Managers

1Password (Demo)

Last Pass

Dashlane

RoboForm (Demo)

What are they?

What are they?

How do I set one up?

Where are my password stored?

How do I share passwords?

Family, spouse, common use

What are the costs?

Good overview at Consumer Reports (<https://www.consumerreports.org/digital-security/everything-you-need-to-know-about-password-managers/>)

XKCD Meme

PASSWORD STRENGTH

I< < PREV RANDOM NEXT > >I

Method 1: Tr0ub4dor &3

UNCOMMON (NON-GIBBERISH) BASE WORD: Tr0ub4dor &3
ORDER UNKNOWN: &3
CAPS?: 0
COMMON SUBSTITUTIONS: 4, &
NUMERAL: 3
PUNCTUATION: &
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

~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**
DIFFICULTY TO REMEMBER: **HARD**

Method 2: correct horse battery staple

FOUR RANDOM COMMON WORDS: correct, horse, battery, staple

~44 BITS OF ENTROPY
 $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$
DIFFICULTY TO GUESS: **HARD**
DIFFICULTY TO REMEMBER: **EASY** (THAT'S A BATTERY STAPLE. CORRECT!)

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.

I< < PREV RANDOM NEXT > >I

PERMANENT LINK TO THIS COMIC: <https://xkcd.com/936/>

IMAGE URL (FOR HOTLINKING/EMBEDDING): https://imgs.xkcd.com/comics/password_strength.png

How big is your haystack?

<https://www.grc.com/haystack.htm>

Demonstrations