

p@ssw0rd\$



Overview

1. Making strong passwords (ft. NIST)
2. Advantage of randomized passwords
3. Password manager solutions
4. 2FA/MFA solutions
5. Passkeys, FIDO



Why is password security important?



Online identity tied to accounts (identity theft)

Easily crackable passwords leads to compromised accounts

And more...

game time



Yell out if each password is good or bad

secret_password



s3cur3_p@ssw0rd



1234567890



G/C=.X]&`SdM7Du8sLwcN!UjWk-hZF{Q3[r



Tr0ub4dor&3



trolled



Yell out if each password is good or bad

secret_password	X
s3cure@secure.com	X
123456	X
G/Cat & `Secure!UjW`hZF{Q3[r	X
Temp4dor&3	X

complicated password \neq good password

How to make good passwords



National Institute of Standards and Technology:

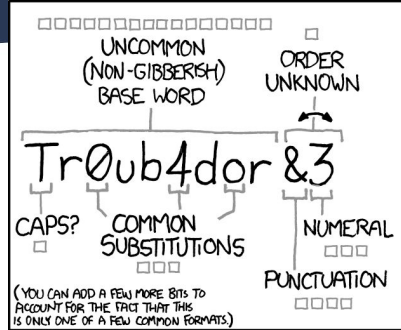
1. Prioritize pw length over complexity

➤ `P@ssw0rd <<< Cyber Security Is My Greatest Passion`

2. Make memorizable passwords

➤ `k>K;.9t5jc(F'mEh[eY8A)aZ?LxzgR` is secure but how are ya gonna remember that

Relevant xkcd



~28 BITS OF ENTROPY

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

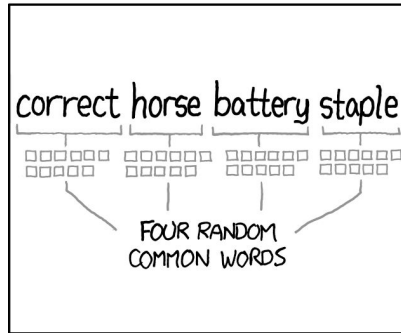
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

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.

(xkcd #936)

Advice



Generate random passwords

- Avoid reusing passwords *more on this later*
- Don't generate garbage

Recommendation: **Diceware Passwords**

Try it out! <https://diceware.dmath.org/>

They may not contain special characters, but they're harder to crack

Why not reuse passwords?



Damage control

- If one account gets breached, your other accounts stay safe

Similar passwords, too

- They are easily brute-forceable using open-source rulesets

Too lazy?

- Let your password manager remember them for you!

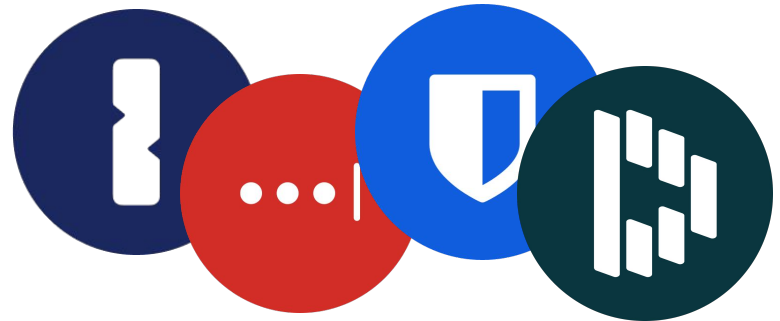
Password managers!



Why

- Backup in case you forget passwords
- Keeps you from typing passwords in public (esp. on a phone)

There's a bunch to choose from



How do pw managers work?



- Create a master password – don't forget it!
- Passwords are encrypted, stored on managers' servers (usually)
- Passwords get autofilled – no one can look over your shoulder!

Password managers have extensions for most web browsers

Note: browser pw managers



Avoid using them!

Ex. Google's password manager





- Uses your Gmail creds to log in → no master password
- By default, passwords aren't encrypted on Google servers
- Extensions can quickly export unencrypted passwords

Simple password/cookies/history/
bookmarks stealer/dumper for chrome all
version (includes 80+), microsoft edge
browser, includes all chromium based
browsers, and all gecko based browser
(firefox etc.).

The most powerful stealer written in
Python 3 and packed with a lot of
features.

Brief overview of pw managers



	1Password 	LastPass 	Bitwarden 	Dashlane 
<i>Entry-level price</i>	\$2.99/month	\$0	\$0	\$0
<i>Unlimited devices for free?</i>	-	✗ (1 device type)	✓	✗ (1 device)
<i>Unlimited passwords for free?</i>	-	✓	✓	✗ (25)
<i>2FA for logging in?</i>	✓	✓	✓	✓

2-factor authentication (2FA)

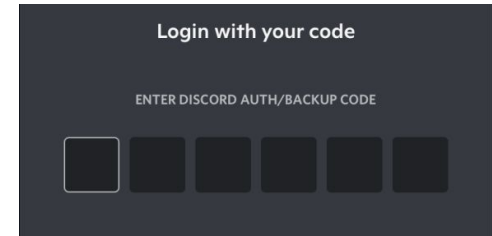


Prevents effectiveness of password cracking

2 step process:

1. Log in using username/password
2. Verify login using email, mobile device, etc.
 - only YOU should have access to this factor

What if you lose your phone?



Codes on an authenticator app refresh every ~30s

2FA backup codes



When you set up 2FA, you have the option to save a list of backup codes

- Backup codes can each be used once
- Use these if you can't use your phone



Moving away from passwords

(passwords are annoying)

Passkeys



Allows you to use biometrics (fingerprint, face, etc.) to sign in

Designed to reduce reliance on passwords

- Cannot be guessed/shared
- Plaintext private keys are not stored on servers
 - safe from breaches

Nothing to memorize – FAR more convenient

Passkeys – Security



Uses asymmetric encryption

One key (public) is used to encrypt, another (private) is used to decrypt

- Public key is stored on app's server – if leaked, no worries
- Private key is kept on user's device OR encrypted + backed up
 - If backed up, key is encrypted using another private key



thanks!

questions questions questions