



PASSWORD MANAGERS



Kevin Adea

Tien-Tso Ning

Abdallah Itani



What are Password Managers?

A password manager is a software application that stores and manages all the passwords a user has for any of their online accounts.

Passwords are encrypted and provide secure access, which can be decrypted using a master password to enter the application.

Extra Features

- Password generator
- Accessible anywhere
- Autofill form
- File Storage

Why Use Password Managers?

- Solution for maintaining and keeping a large amount of passwords and account information
- Prevents needing to remember multiple passwords
 - Automatic password generation
 - You need unique and strong passwords for each account, password manager will do that for you

Justification

- People are lazy and hackers know it
- People don't have the brain power to remember all of the passwords
 - Average user has 200 accounts, and will double within 5 years
- People are bad password generators

UNIGE User

- Gmail
- UNIGE Mail
- LinkedIn
- Youtube
- Microsoft
- Reddit
- Twitter
- Facebook
- Twitch
- Twitter
- Steam
- Riot
- ~~Blizzard~~
- Epic Games
- Amazon
- Ebay

Why Use Password Managers?

- Stores the login information and automatically enters them in the forms
 - Prevents hacker attacks like keystroke logging
 - Automatic form filling that fills in login info whenever you load the URL to a website with an account
 - They can identify the correct pair of URL with login info, so they protect credentials from phishing sites

Type of Password Managers

- Web browser based
- Cloud based
- Desktop
- Portable

Web-Browser Based

Advantages

- Simple
- Syncs across devices
- Convenient
 - “Would you like to store this login for...?”

Disadvantages

- More weight on convenience than security
- Not many features
- The moment someone has access to your personal device they can see your stored passwords

Cloud Based

Advantages

- Stored on the cloud
- Can be accessed from anywhere

Disadvantages

- Security is in service provider's hands

Desktop Based

Advantages

- Stored locally on desktop machine (Safer)
- Can generate passwords for you

Disadvantages

- Cannot be accessed from other machines and devices

Portable Based

Advantages

- Even more secure than desktop based because it is only connected when needed

Disadvantages

- It is a physical device. Can be lost, stolen, or break easily.

Most Widely-Used Managers

- LastPass: Browser/Cloud Based
 - Free, Premium for \$3/month
- 1Password: Cloud Based
 - \$3/month
- Bitwarden*: Browser/Desktop/Cloud Based
 - Free, Premium for \$10/year
- Keeper: Cloud Based
 - Free, Premium for \$4.70/month
- KeePassXC*: Desktop Based
 - Free

*Open Source

LastPass

- AES-256 bit encryption
 - PBKDF2 SHA-256
- Encrypted and decrypted at the device level.
 - LastPass has no access to your data

| FEATURES | FREE | PREMIUM |
|--------------------------------|------|---------|
| 📄 Emergency access | ⊗ | ✓ |
| 📄 One-to-many sharing | ⊗ | ✓ |
| 📄 Advanced multifactor options | ⊗ | ✓ |
| 📄 Priority tech support | ⊗ | ✓ |
| 📄 LastPass for Applications | ⊗ | ✓ |
| 📄 1 GB encrypted file storage | ⊗ | ✓ |

The background consists of a solid pink upper half and a solid dark gray lower half, separated by a jagged horizontal line. The pink section has a small triangular notch pointing downwards into the dark gray section.

Password Entropy

What is it

- Entropy is a way to express the unpredictability of a character or string, Password entropy is a measurement of how unpredictable a password is.
- It's basically the randomness of the password.
- A password with high entropy is theoretically harder to crack through attacks like [brute force](#) cracking, [dictionary attacks](#) or other common methods.
- In order for a password to be completely secure, it must be as random truly random.
- The entropy of a password is typically stated in terms of bits:
 - A known password has 0 bits of entropy.
 - A password with 1 bit of entropy would be guessed on the first attempt 50% of the time.
 - A password with n bits of entropy can be found in 2^n attempts.

The problem with passwords

- People are notoriously poor at achieving sufficient entropy to produce satisfactory and secure passwords; humans are bad password generators.
- Most of the general public still use weak passwords and use the same password across multiple accounts and platforms, even when protecting valuable data or assets.
- Even If patterned choices are required, humans are likely to use them in predictable ways (capitalizing the first letter, adding numbers in the end).

The formula



- A password's entropy can be calculated by finding the entropy per character, which is a \log_2 of the number of characters in the character set used, multiplied by the number of characters of the password.
in the password itself.
- Entropy = $\log_2(\text{\# of available characters}) * \text{Length}$
- Its \log_2 since a password with entropy n can be cracked in 2^n attempts

What can users do

- It's better not to rely on a single password for accessing, sensitive data, accounts that involve money and assets, or even your password management system.
- Use Password managers that set us up with highly entropic passwords. They have a good random number generator that is truly unpredictable, and its what users need.
- Password management systems help also in storing the passwords with encryption and manage passwords across multiple accounts.
- Chrome already has a basic password manager built in.

Securing Your Credentials

- Step 1: Knowing if you have vulnerabilities
- Does your password have enough entropy?
- Do you store your data well?
- Do the companies that have your data secure your data well?
- Check if you were part of a data-breach: <https://haveibeenpwned.com/>

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate](#)  

';--have i been pwned?

Check if you have an account that has been compromised in a data breach



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

Securing Your Credentials

- Step 2: Preventing password reuse
- How many passwords can you remember?
- How many of those passwords have good enough entropy?
- Example: "nWS67H%waxyb" 12 char
- Example: "tinygoblinpeoplehaveme" 22 char (from xkcd's "Password Strength"
<https://xkcd.com/936/>)
- But eventually you will forget.

Securing Your Credentials

- Step 3: Understanding risks
- Nothing is perfect.
- You won't remember everything.
- How much do you have to lose/Are you worth attacking?
- Even if you're perfect, is this how you want to live your life?

Securing Your Credentials

- Step 5: Use the features, and additional help from 2FA
- Password generation
- What is “random?” How random is it? (True vs Pseudo) Do we know?
- Radioactive Decay/physical phenomenon vs seeding
- Hardware mixed with algorithmic solutions
- But in the end, passwords are not the end-all-be-all