Password Managers

Marina Moshchenko, Iulian J Irimina

Why password managers

- Passwords are old technology that doesn’t seem to be replaced in the near future
- Some studies point to the fact that secure passwords are difficult to remember and users have difficulty matching their passwords to accounts
- Experts recommend you do not reuse passwords
- Some websites still require users to create login questions to help with user authentication.

Common Security Questions

- What Is your favorite book?
- What is the name of the road you grew up on?
- What is your mother’s maiden name?
- What was the name of your first/current/favorite pet?
- What was the first company that you worked for?
- Where did you meet your spouse?
- Where did you go to high school/college?
- What is your favorite food?
- What city were you born in?
- Where is your favorite place to vacation?

- Using questions like these, researchers at Microsoft and Carnegie Mellon found that people with no knowledge of the person whose account they were hacking were able to guess the correct answer 15% of the time.
- the majority of these questions are topics that are discussed on a first date and are common material for social network profiles and updates.
- How Identity Thieves Get The Answers to Your Computer Security Questions

What is a password manager

- Password managers represent a possible solution that addresses the issues of memorability and keeping track of of passwords.
- Passwords managers help you generate unique and strong passwords and store them in one safe (encrypted) place,
- You only need to remember one master password.
- The master password unlocks your encrypted vault which grants you access to each of your passwords.

Local Password Management

- Password managers are able to store your passwords locally on your computer or in the cloud
- Password managers have become more convenient to users through browser extensions and native apps for your mobile devices.
- Storage hampers the user experience but forces hackers to resort to difficult malware-based approaches like using keyloggers and other advanced tools. (Carnegie-Mellon University)
- Since the password is stored on the user's device, the user has total control over its security.

Cloud Storage

- Encrypted passwords are stored in a server which provides the convenience of access them from any device
- Storage improves accessibility makes passwords recoverable if the user loses the device.
- However, the user cannot ensure the security of data and breaches happened in the past
- However, if a password manager stores all your passwords in an encrypted format, and your master password only as a "hash" that's the result of an irreversible mathematical process. (Carnegie-Mellon University)

1Password

Platforms: Windows, Mac, iOS, Android, **1Password X Platforms:** Linux, Chrome OS

Free-version Limitations: Single mobile device

Two-Factor Authentication: Yes

Browser plugins: Chrome, Firefox, IE, Safari, Edge, Opera

Form Filling: Yes

Mobile App PIN Unlock: Yes

Biometric Login: Face ID, Touch ID on iOS & macOS, most Android fingerprint readers

Storage Option: Locally or Online (Cloud)

Price: Individual Plan-$36/year, Family Plan- $60/year

- No free version but it allows for a 1 month free trial
- It features the service **Watchtower**, which notifies you if you have an account that may have been compromised (based on the URL and news reports), a weak password, or even a reused password.

Apple's iCloud Keychain

Platforms: Mac, iOS

Free-version Limitations: N/A

Two-Factor Authentication: Yes

Browser plugins: Safari

Form Filling: Yes

Mobile App PIN Unlock: If

Biometric Login: Face ID, Touch ID on iOS & macOS

Storage Option: Cloud

Price: Free

- It allows you to sync and share your passwords between any Apple device that you are logged into using your iCloud account.
- If a user has multiple devices, or two-factor authentication for iCloud is enabled, key recovery is accomplished by using another device. If a user has a single Apple device, Apple provides an optional key recovery (escrow) service that allows Apple to have access to decrypt your keychain under certain circumstances.

KeePass

Platforms: Windows, Mac, iOS, Android, Linux

Free-version Limitations: N/A

Two-Factor Authentication: Yes

Browser plugins: None

Form Filling: No

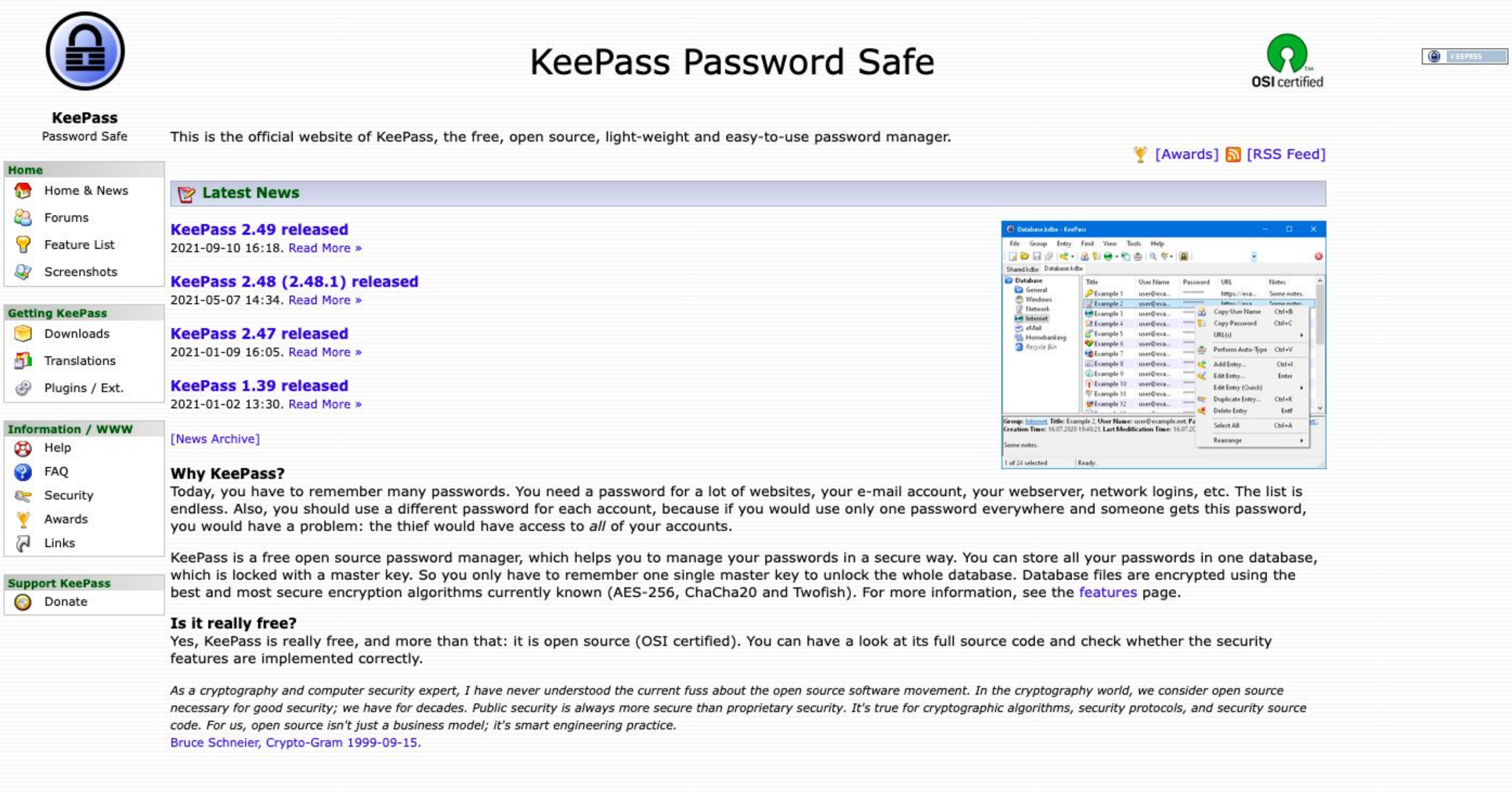
Mobile App PIN Unlock: Depends on version

Biometric Login: Depends on version

Storage Option: Local

Price: Free

- It offers local storage option storing passwords on your laptop, desktop, or mobile device.
- KeePass is open source, and the source code is available for your review.
- Highly technical, open-source nature can be intimidating



KeePass Password Safe

KeePass
Password Safe

OSI certified

This is the official website of KeePass, the free, open source, light-weight and easy-to-use password manager.

[Awards] [RSS Feed]

Home
- Home & News
- Forums
- Feature List
- Screenshots

Getting KeePass
- Downloads
- Translations
- Plugins / Ext.

Information / WWW
- Help
- FAQ
- Security
- Awards
- Links

Support KeePass
- Donate

Latest News

KeePass 2.49 released
2021-09-10 16:18. Read More »

KeePass 2.48 (2.48.1) released
2021-05-07 14:34. Read More »

KeePass 2.47 released
2021-01-09 16:05. Read More »

KeePass 1.39 released
2021-01-02 13:30. Read More »

[News Archive]

Title	User Name	Password	URL	Notes
Example 1	user@exa...	********	https://exa...	Some notes.
Example 2	user@exa...	********	https://exa...	Some notes.
Example 3	user@exa...	*****		
Example 4	user@exa...	*****		
Example 5	user@exa...	*****		
Example 6	user@exa...	*****		
Example 7	user@exa...	*****		
Example 8	user@exa...	*****		
Example 9	user@exa...	*****		
Example 10	user@exa...	*****		
Example 11	user@exa...	*****		
Example 12	user@exa...	*****		

Group: Internet, **Title:** Example 2, **User Name:** user@example.net, **Pa**
Creation Time: 16.07.2020 19:40:23, **Last Modification Time:** 16.07.20

Some notes.

1 of 24 selected | Ready.

Why KeePass?

Today, you have to remember many passwords. You need a password for a lot of websites, your e-mail account, your webserver, network logins, etc. The list is endless. Also, you should use a different password for each account, because if you would use only one password everywhere and someone gets this password, you would have a problem: the thief would have access to *all* of your accounts.

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. You can store all your passwords in one database, which is locked with a master key. So you only have to remember one single master key to unlock the whole database. Database files are encrypted using the best and most secure encryption algorithms currently known (AES-256, ChaCha20 and Twofish). For more information, see the features page.

Is it really free?

Yes, KeePass is really free, and more than that: it is open source (OSI certified). You can have a look at its full source code and check whether the security features are implemented correctly.

As a cryptography and computer security expert, I have never understood the current fuss about the open source software movement. In the cryptography world, we consider open source necessary for good security; we have for decades. Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code. For us, open source isn't just a business model; it's smart engineering practice.
Bruce Schneier, Crypto-Gram 1999-09-15.

LastPass

Platforms: Windows, Mac, iOS, Android, Linux, Chrome OS, Windows Phone, watchOS

Free-version Limitations: Limited password sharing, limited 2FA

Two-Factor Authentication: Yes

Browser plugins: Chrome, Firefox, IE, Safari, Edge, Maxthon, Opera

Form Filling: Yes

Mobile App PIN Unlock: Yes

Biometric Login: Face ID, Touch ID on iOS & macOS, most Android & Windows fingerprint readers

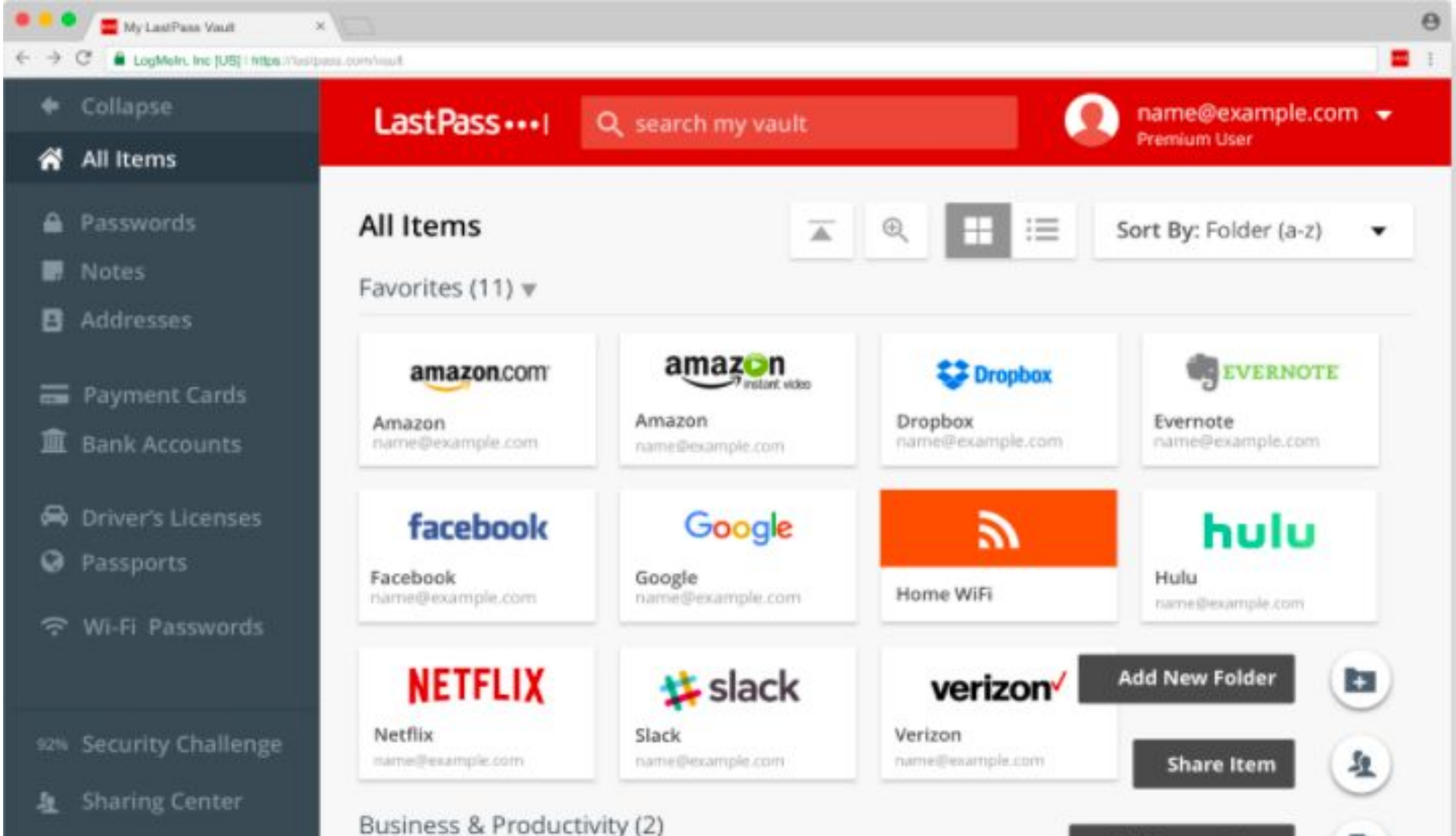
Storage Option: Cloud

Price: Free (Premium Plan-$36/year, Family Plan- $48/year)

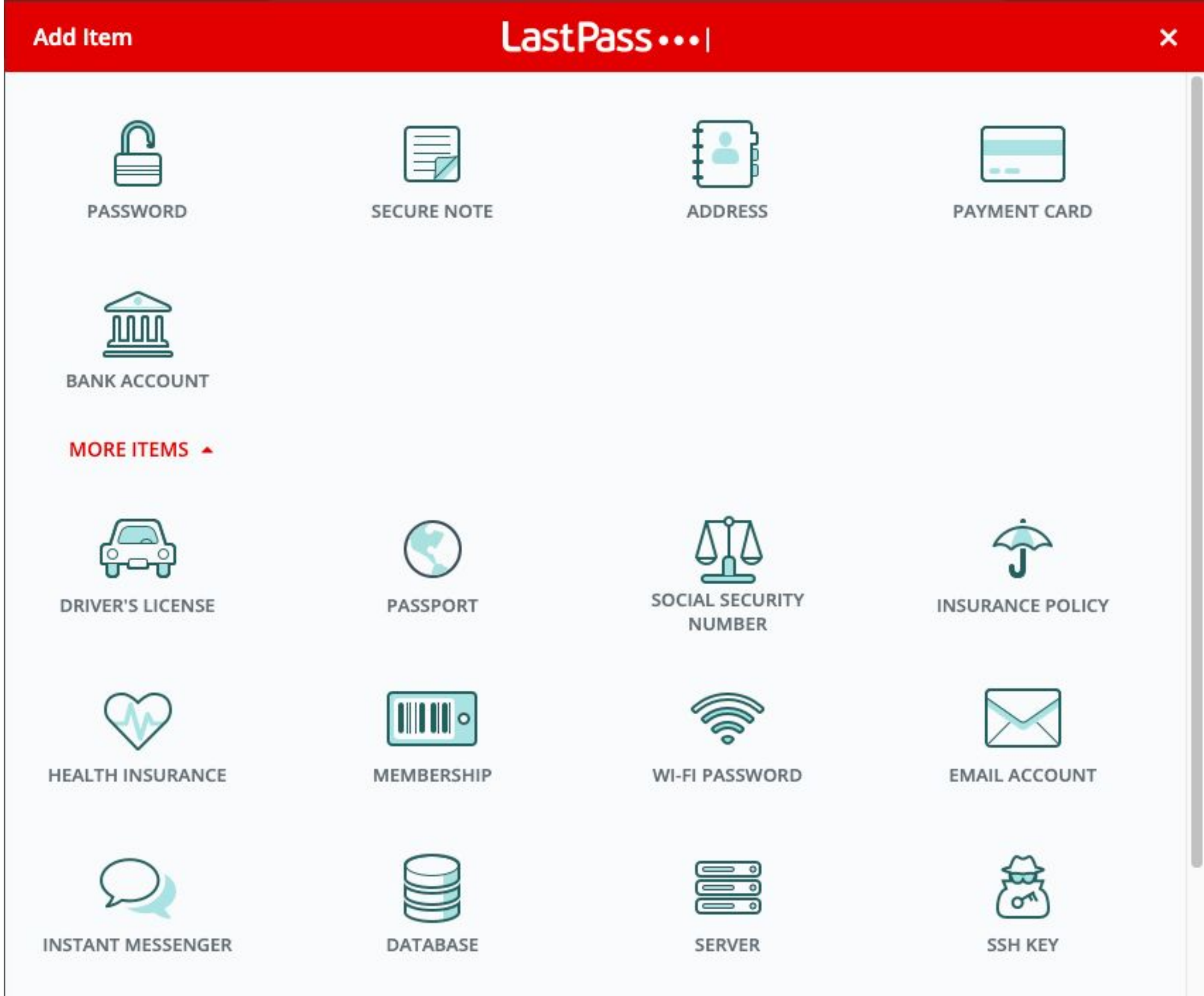
LastPass

- The premium users benefit from dark web monitoring and alerts them if any of their email addresses/accounts have been compromised
- Tech Support only for Premium members

- 2015 Security Breach, 2017 & 2019 Reported Security Vulnerability (did not affect user passwords/accounts)

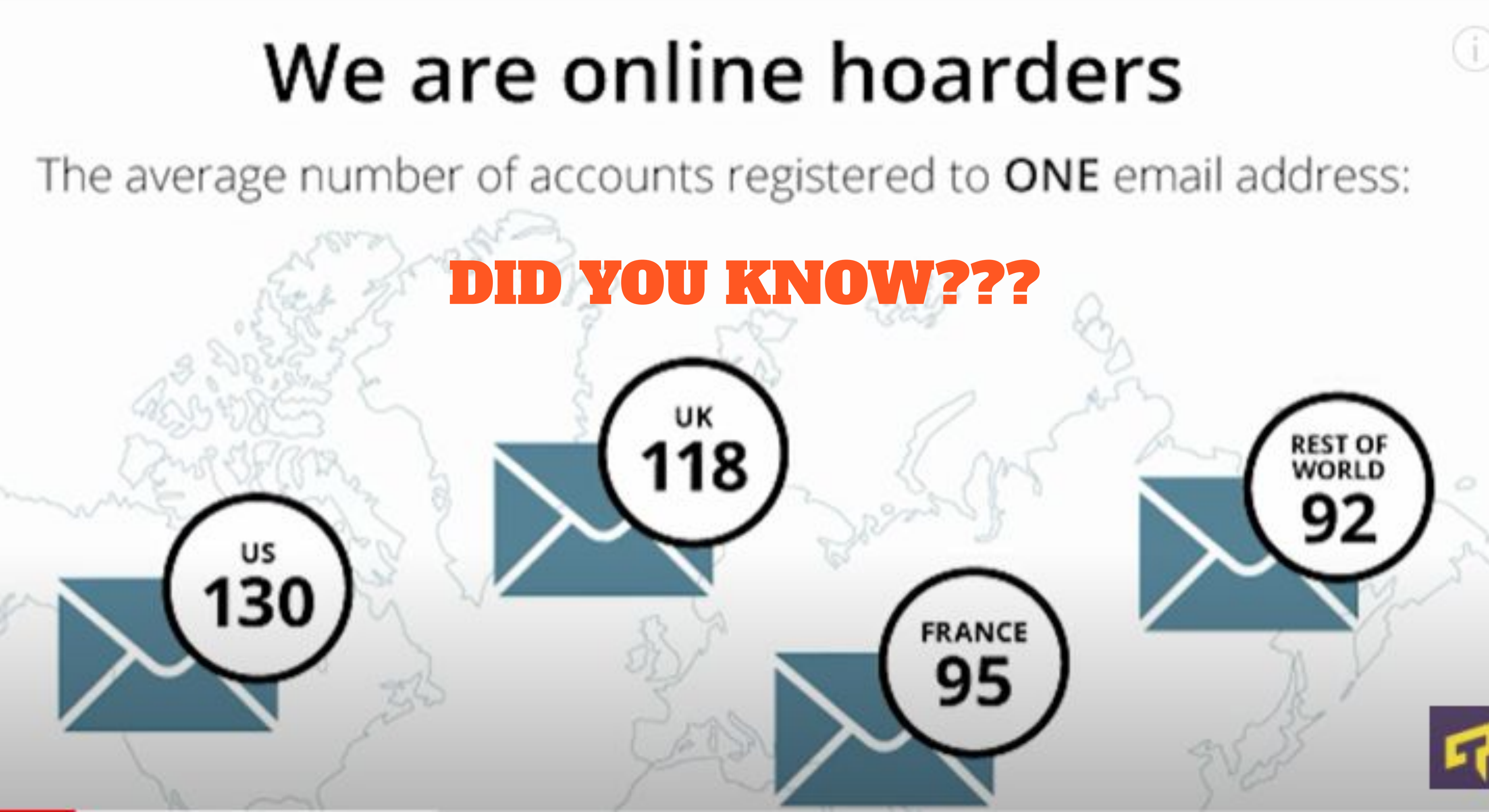

My LastPass Vault
LogMeIn, Inc [US] | https://lastpass.com/vault
Collapse
All Items
Passwords
Notes
Addresses
Payment Cards
Bank Accounts
Driver's Licenses
Passports
Wi-Fi Passwords
92% Security Challenge
Sharing Center
LastPass•••|
search my vault
name@example.com
Premium User
All Items
Sort By: Folder (a-z)
Favorites (11)
Amazon
name@example.com
Amazon
name@example.com
Dropbox
name@example.com
Evernote
name@example.com
Facebook
name@example.com
Google
name@example.com
Home WiFi
Hulu
name@example.com
Netflix
name@example.com
Slack
name@example.com
Verizon
name@example.com
Add New Folder
Share Item
Business & Productivity (2)

Other info you can store



Google Password Manager

Is not recommended for storage and syncing using Chrome as Google has access to your unencrypted passwords. (Carnegie Mellon)



We are online hoarders

The average number of accounts registered to **ONE** email address:

DID YOU KNOW???

US
130

UK
118

FRANCE
95

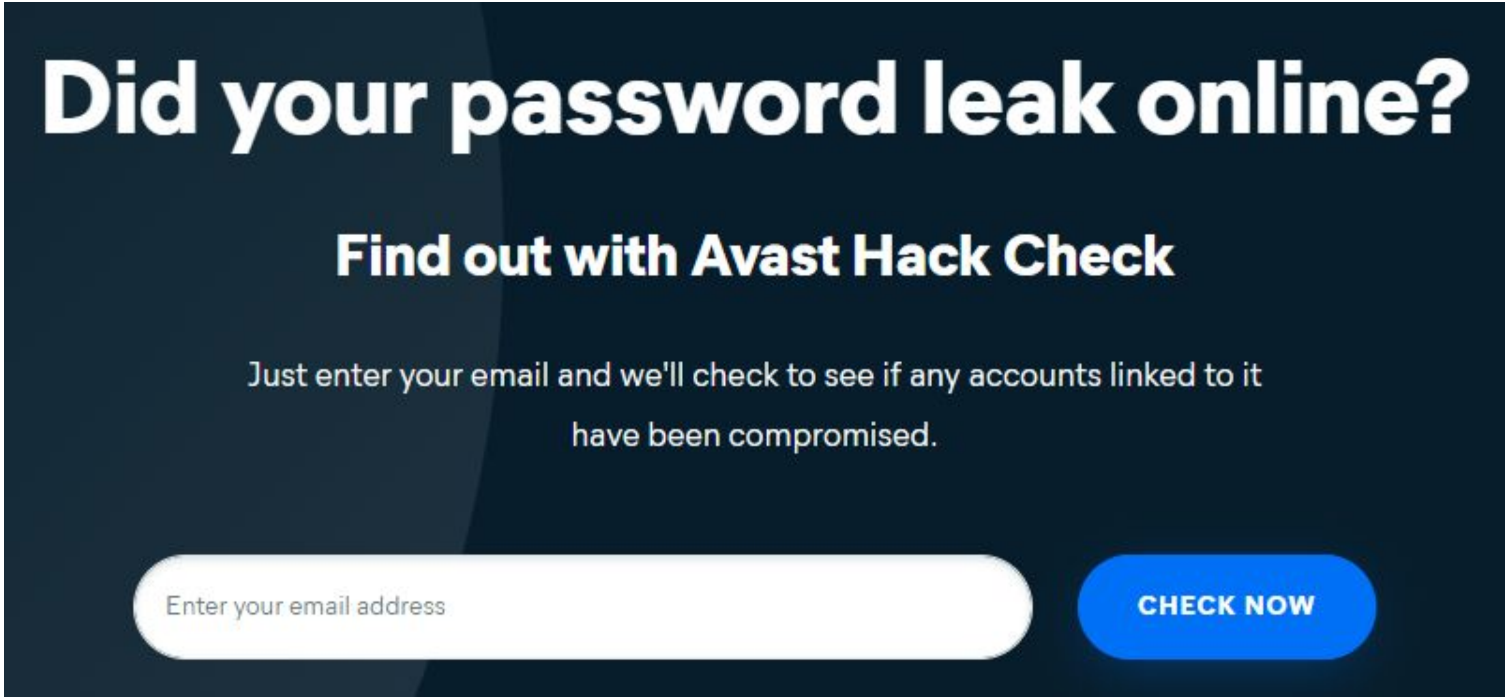
REST OF WORLD
92

DID YOU KNOW???

1. Roughly **6.85 million** accounts get hacked every single day
2. **51 percent** of people utilize the same passwords for personal and work accounts
3. About **23 million** people still secure online accounts with a simple password like 123456

Did your password leak online?

https://www.avast.com/hackcheck/



Did your password leak online?

Find out with Avast Hack Check

Just enter your email and we'll check to see if any accounts linked to it have been compromised.

Can password managers get hacked? YES!

As any other application...

The vast majority of cyber-security specialists agree that password managers are indeed the most secure way to protect your passwords.

PM PROS

- Humans can be unreliable as they can come up with bad passwords, forget their password, or are genuinely disinterested in security. With a PM there is **no need to worry about remembering all your different passwords**.
- Using the **same credentials for each account is dangerous** as it creates one point of failure.
- Good password managers **encrypt all your personal data** in case someone hacks the PM software directly; the hacker might get your passwords but they **won't know who the passwords belong to**.
- PMs can keep you **up to date with the latest breaches** and advise you if any accounts may have been affected/hacked.
- Can use **offline password manager** (not stored on the web/not a web browser plugin).

PM CONS

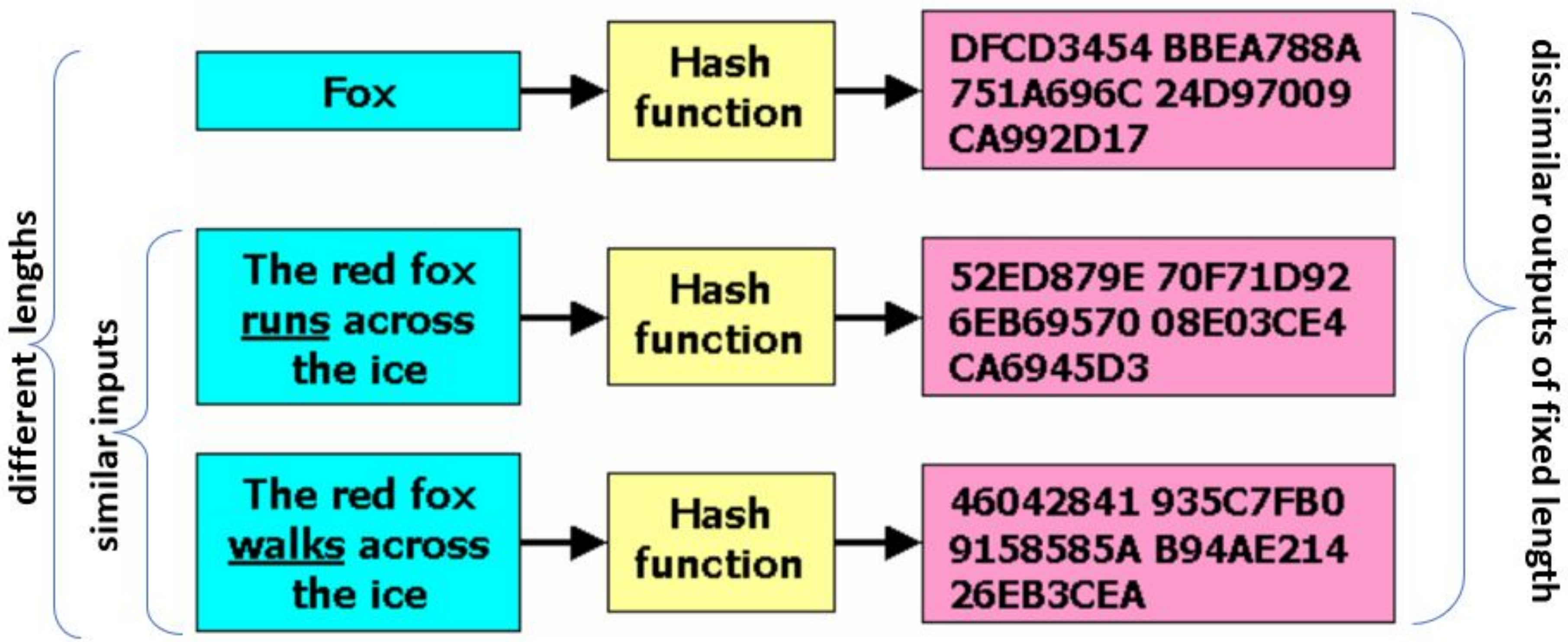
- **Single point of failure** - if someone gets hold of your master password, they have all your passwords.
- Password manager programs are a **target for hackers**.
- It's **not easy to login** using multiple devices.
- If the main password is used/typed/saved on a **computer with malware**, your main password can compromise all your other passwords controlled by the PM - **all your passwords are only as secure as your master password**.
- **Not all PM's are adequately encrypted** which can render the whole process of setting one up useless.
- **Password Manager breach**.

Common Password Encryption & Hash Formats

Password example: R@nT4g*Ne!

FORMAT	DESCRIPTION	SECURE PASSWORD (EXAMPLE)
SHA-1	Password is made up of **40 hexadecimal characters**, and there is no clear decryption method. 160 bits	12bf203295c014c580302f4fae101817ec085949
SHA-1 with Salt	Password is still made up of **40 hex characters**, but we appended the word "Free." 160 bits	bc6b79c7716722cb383321e40f31734bce0c3598
MD5 Message Digest	Password is encoded into a 128-bit string. This tool provides a quick and easy way to encode an MD5 hash from a simple string of up to 256 characters in length - **32 hex characters.** Widely used. Collisions possible.	4e84f7e8ce5ba8cdfe99d4ff41dc2d41
SHA256	Password is encoded into a 256-bit string. Created by the National Security Agency in 2001 as a successor to SHA-1. Data may be of unlimited size **64 hex characters.** Widely used. Slower than MD5.	5fd0c5bebb6481579f9028b3dfa7bed982e30830315072a803197e83067224db
SHA512 Secure Hash Algorithm	Secure Hash Algorithm 512, is a hashing algorithm used to convert text of any length into a fixed-size string. Each output produces a SHA-512 length of 512 bits (64 bytes) **128 hex characters.** Not widely used yet.	d3b21eeeb5b6c20a54d8cd2b0a2e16ab9e572dd0b1b181b174783e38c9d0fa1b0f6da952be405b35e232d7e6914bca10a4feb8815797a3d1cb3b119f02764528
AES Advanced Encryption Standards	With this symmetric encryption algorithm, you can choose bit length. It's nearly impossible to model what our completed password might look like, as we have far too many variables to choose from, and each will impact the outcome. Used to scramble data while in transit and unscramble it when it reaches the legitimate destination.	Nearly impossible to model due to multiple variables

Secure Hash Algorithm



different lengths

similar inputs

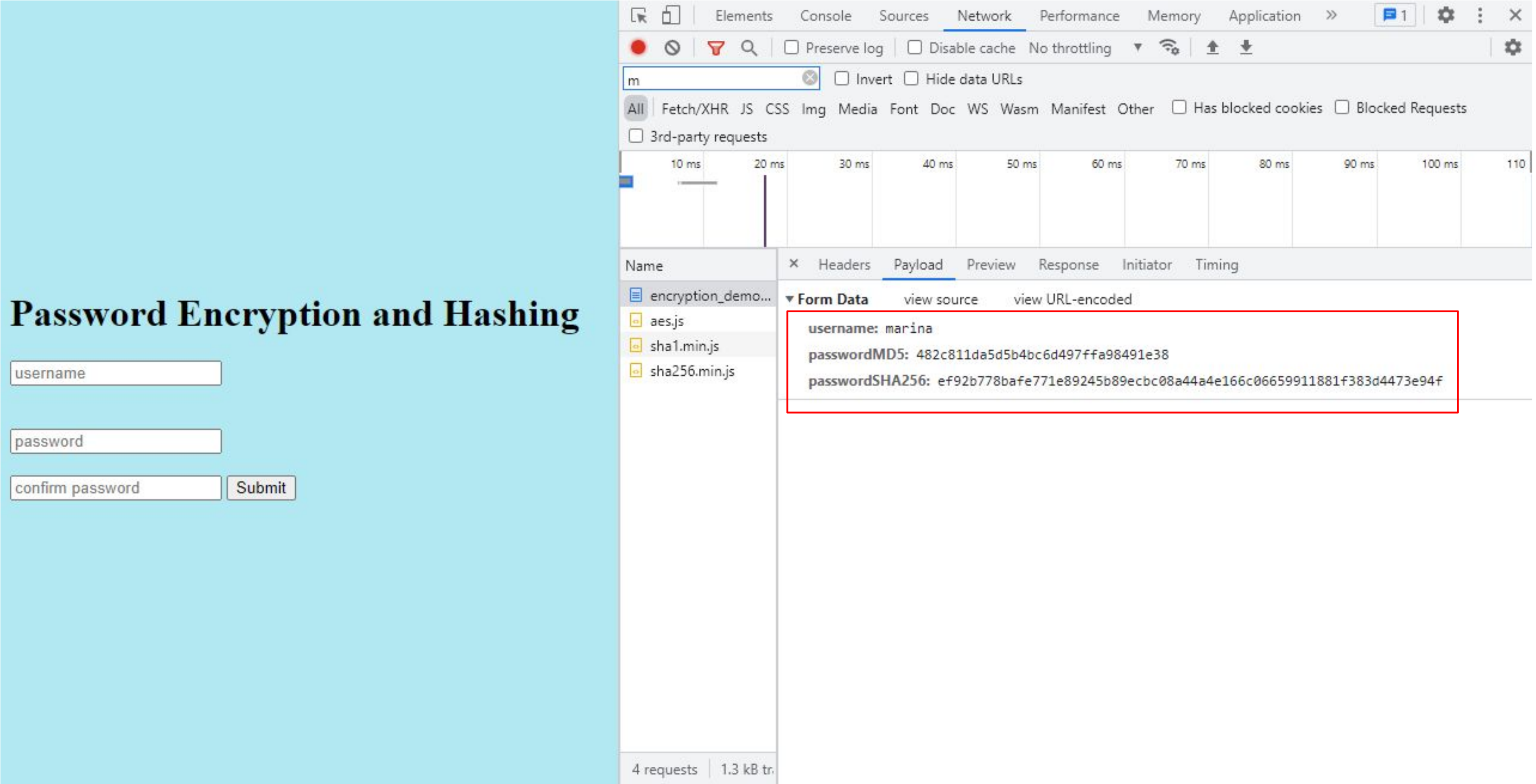
Fox → Hash function → DFCD3454 BBEA788A 751A696C 24D97009 CA992D17

The red fox **runs** across the ice → Hash function → 52ED879E 70F71D92 6EB69570 08E03CE4 CA6945D3

The red fox **walks** across the ice → Hash function → 46042841 935C7FB0 9158585A B94AE214 26EB3CEA

dissimilar outputs of fixed length

Coding Sample



Password Encryption and Hashing

▼ Form Data

```
username: marina
passwordMD5: 482c811da5d5b4bc6d497ffa98491e38
passwordSHA256: ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
```

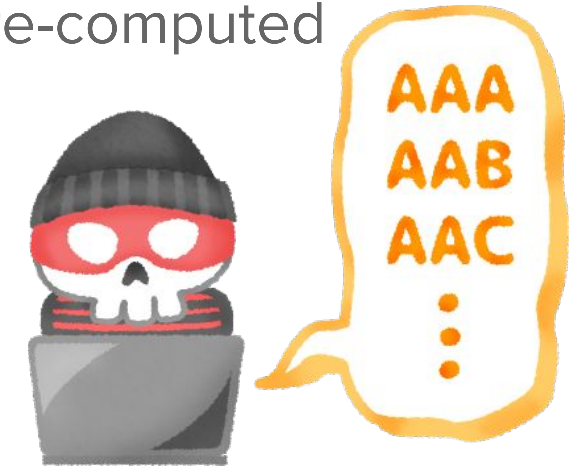
How to crack a hashing system

1. Steal a list of hashed passwords from a server
2. Pick a password attempt
3. Hash it
4. Compare the hashed result with all of the hashes in the stolen database.
5. If you find a match, you have guessed one password

Or decrypt (and encrypt) up to 100 hashes :
https://md5decrypt.net/en/#answer

How to brute force in record time (Rainbow Tables)

1. Start with a dictionary of million common passwords
2. Hash each word (may take many days to compute the entire list)
3. Store the password and its hash in a (very large) database
4. Quickly apply brute force methods using pre-computed values
5. Download your own rainbow tables here… http://project-rainbowcrack.com/table.htm



How to defeat Rainbow Tables?

Best:

SALTING A PASSWORD - add unique number before the password and then hash it. So that way it does not fit into anybody’s precomputed or rainbow tables.

OR

MULTIPLE ROUNDS OF HASHING (repeat an algorithm multiple times)

Can I create my own password manager? YES!

1. Choose a hash algo easily used by the language and IDE of your choice.
2. Use it to hash your master password. (you can also create the add, update, reset master password features here; you can also add 2 factor auth with google authenticator)
3. Store the hash for verification. Even if someone has your password, they would not break the hash in reverse.
4. Create record table with portal, username, and password fields.
5. For each record you add, generate a random password (8 characters or more long) using a combination of uppercase, lowercase, numbers, and symbols (@ works on most portals)
6. Ensure that you do not update an existing record for the same. For safety, just use add and delete features. (make deletion harder with multiple confirmations and requiring master password)
7. Encrypt the records file. (different from hashing as you will decrypt it to use e.g. multiply a number by 5 to encrypt, divide by 5 to decrypt)
8. Use the random passwords on your logins. You are done.
9. (Optional) You can sync your encrypted records file to google drive to allow you to use the file on multiple devices.

Resources

https://www.cmu.edu/iso/governance/guidance/password-managers.html

https://stumbleforward.com/2012/08/20/the-10-most-common-password-security-questions/

https://cheatsheetseries.owasp.org/cheatsheets/Choosing_and_Using_Security_Questions_Cheat_Sheet.html

https://www.acm.org/articles/people-of-acm/2016/lorrie-cranor

https://dl.acm.org/doi/10.1145/3412841.3442131

https://www.youtube.com/watch?v=GI790E1JMgw

https://us.norton.com/internetsecurity-privacy-password-manager-security.html

https://us.norton.com/internetsecurity-privacy-password-manager-security.html

https://expert.services/blog/managing-your-website/security/password-managers