UNIVERSITY OF
TORONTO

Exploring Self-Hosted Password Managers

Benefits & drawbacks of using password managers

Norbert Krawiec (SciNet)

May 24, 2023

UNIVERSITY OF TORONTO

What is a password manager?

A software application designed to securely store different types of information

Password managers generate strong, unique passwords for each online account and store them in an encrypted vault.

Password managers can store passwords, secure notes and important pictures, credit cards, passports information, etc.

Some password managers allow you to share passwords in secure fashion between family members or wo-workers.

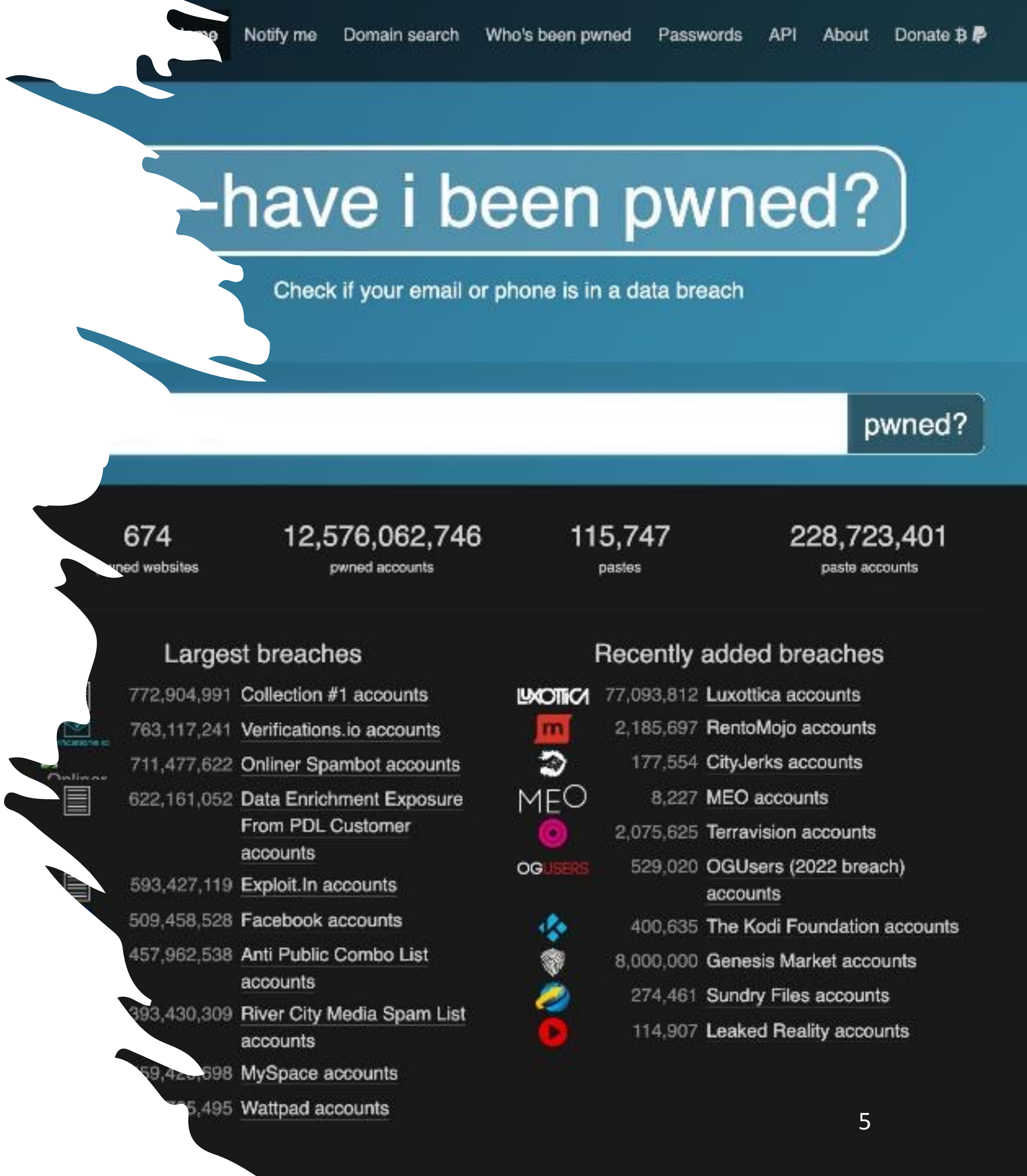
Benefits of using password managers 👍

- **Only 1 password** – you only need to remember 1 password vs. multiple passwords
- **Stronger security** – they generate complex, unique passwords that are resistant to brute-force attacks
- **Enhanced privacy** – they store passwords locally or in the cloud with encryption, reducing the risk of data breaches
- **Time-saving** – they have an auto-fill feature for login credentials on websites and apps, saving time and effort.

Why should you use a password manager?

Hacked accounts

- Go to this website https://haveibeenpwned.com/
- Enter your email
- See if you've been pwned



have i been pwned?

Check if your email or phone is in a data breach

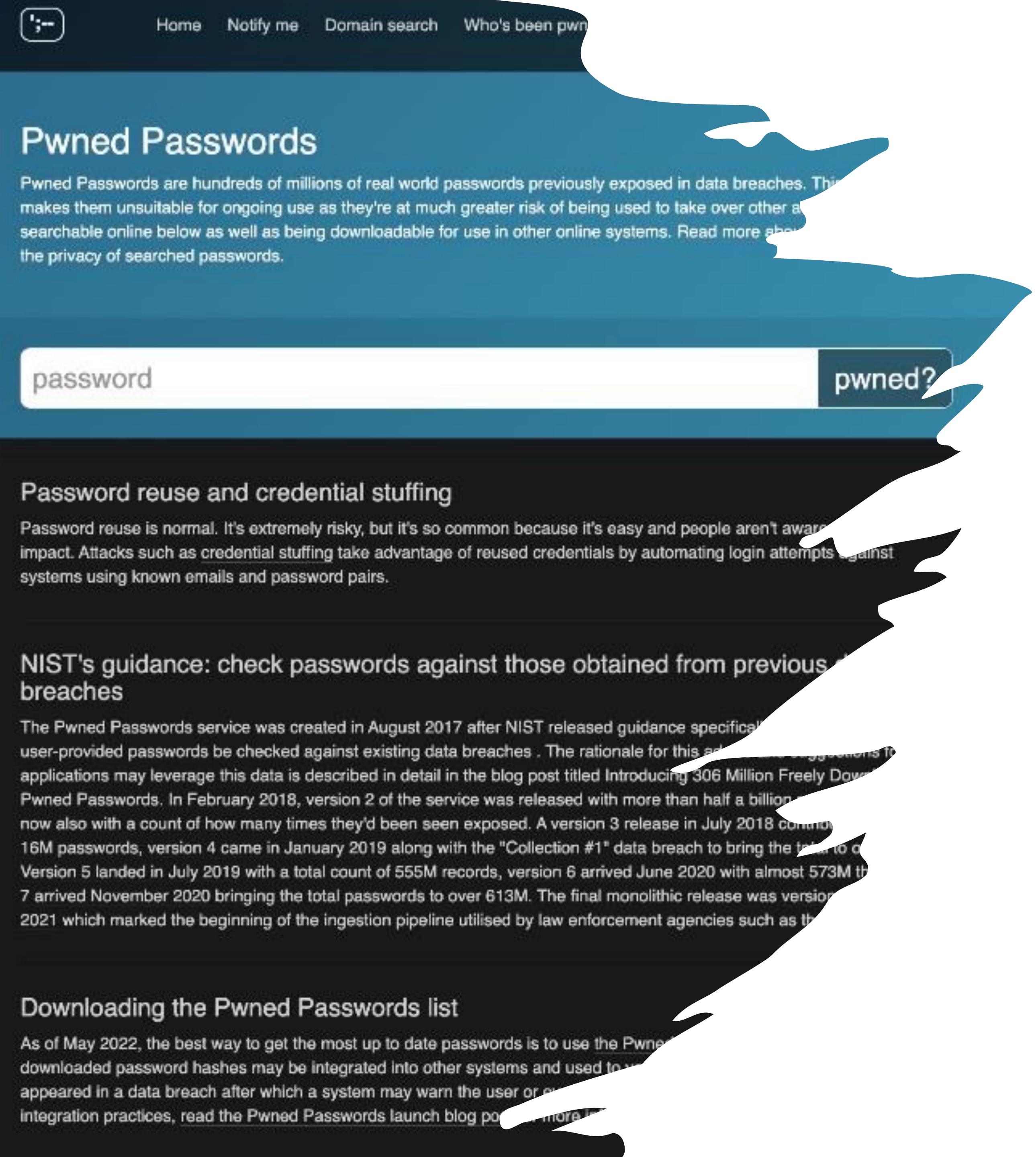
674	12,576,062,746	115,747	228,723,401
ned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
59,42[illegible]698	MySpace accounts
[illegible]5,495	Wattpad accounts

Recently added breaches

LUXOTTICA	77,093,812	Luxottica accounts
m	2,185,697	RentoMojo accounts
	177,554	CityJerks accounts
MEO	8,227	MEO accounts
	2,075,625	Terravision accounts
OGUSERS	529,020	OGUsers (2022 breach) accounts
	400,635	The Kodi Foundation accounts
	8,000,000	Genesis Market accounts
	274,461	Sundry Files accounts
	114,907	Leaked Reality accounts



Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. Thi
makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other a
searchable online below as well as being downloadable for use in other online systems. Read more abou
the privacy of searched passwords.

Password reuse and credential stuffing

Password reuse is normal. It's extremely risky, but it's so common because it's easy and people aren't aware
impact. Attacks such as credential stuffing take advantage of reused credentials by automating login attempts against
systems using known emails and password pairs.

NIST's guidance: check passwords against those obtained from previous
breaches

The Pwned Passwords service was created in August 2017 after NIST released guidance specifical
user-provided passwords be checked against existing data breaches . The rationale for this a
applications may leverage this data is described in detail in the blog post titled Introducing 306 Million Freely Dow
Pwned Passwords. In February 2018, version 2 of the service was released with more than half a billion
now also with a count of how many times they'd been seen exposed. A version 3 release in July 2018 contrib
16M passwords, version 4 came in January 2019 along with the "Collection #1" data breach to bring the total to o
Version 5 landed in July 2019 with a total count of 555M records, version 6 arrived June 2020 with almost 573M th
7 arrived November 2020 bringing the total passwords to over 613M. The final monolithic release was versio
2021 which marked the beginning of the ingestion pipeline utilised by law enforcement agencies such as th

Downloading the Pwned Passwords list

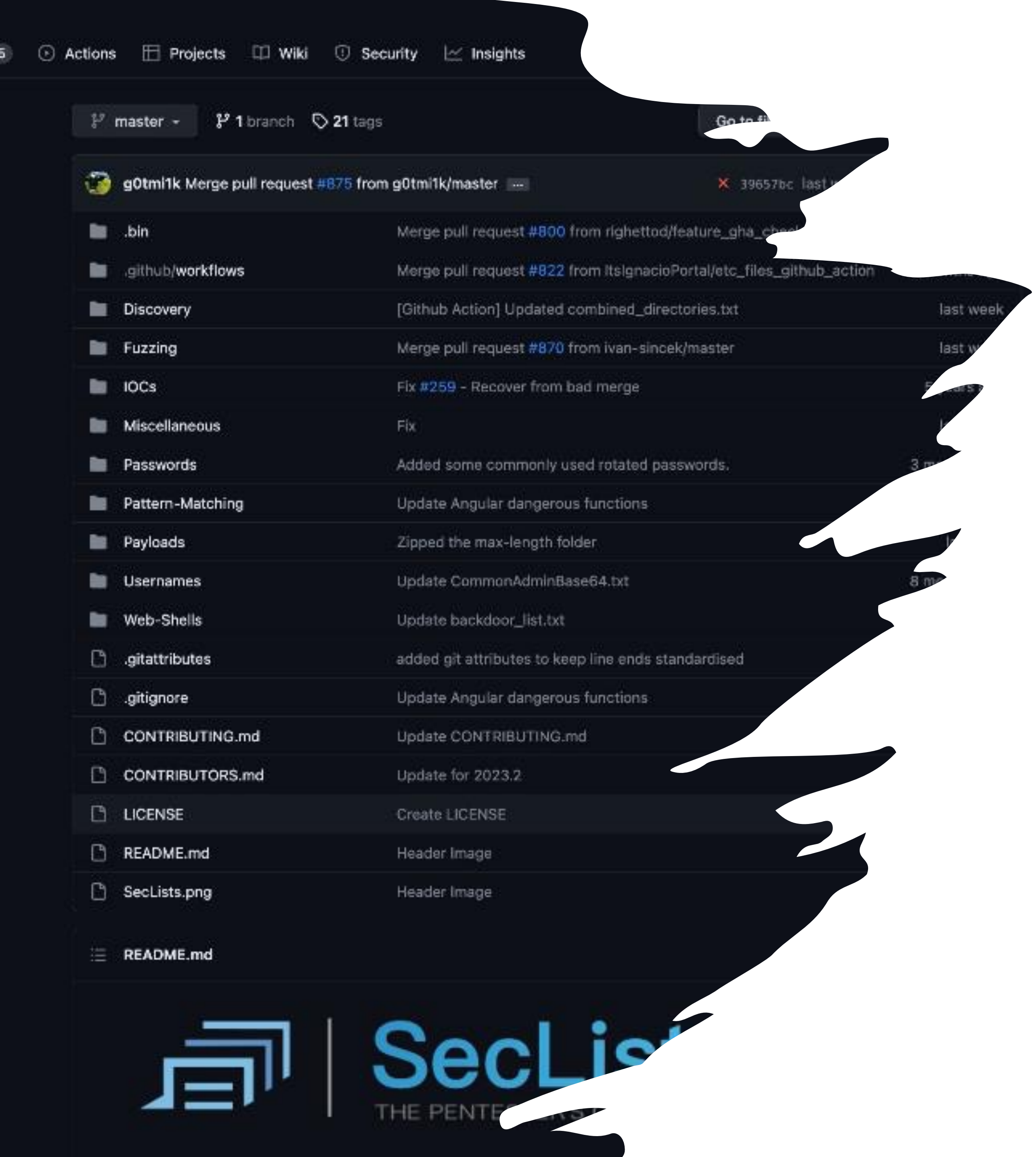
As of May 2022, the best way to get the most up to date passwords is to use the Pwne
downloaded password hashes may be integrated into other systems and used to v
appeared in a data breach after which a system may warn the user or
integration practices, read the Pwned Passwords launch blog po more in

UNIVERSITY OF TORONTO

Hacked passwords

- Go to this website https://haveibeenpwned.com/Passwords
- Enter your password
- See if your password is in an open database

SciNet



g0tmi1k Merge pull request #875 from g0tmi1k/master ... 39657bc last

.bin	Merge pull request #800 from righettod/feature_gha_chec	
.github/workflows	Merge pull request #822 from ItsIgnacioPortal/etc_files_github_action	
Discovery	[Github Action] Updated combined_directories.txt	last week
Fuzzing	Merge pull request #870 from ivan-sincek/master	last w
IOCs	Fix #259 - Recover from bad merge	
Miscellaneous	Fix	
Passwords	Added some commonly used rotated passwords.	3 m
Pattern-Matching	Update Angular dangerous functions	
Payloads	Zipped the max-length folder	
Usernames	Update CommonAdminBase64.txt	8 m
Web-Shells	Update backdoor_list.txt	
.gitattributes	added git attributes to keep line ends standardised	
.gitignore	Update Angular dangerous functions	
CONTRIBUTING.md	Update CONTRIBUTING.md	
CONTRIBUTORS.md	Update for 2023.2	
LICENSE	Create LICENSE	
README.md	Header Image	
SecLists.png	Header Image	

README.md

UNIVERSITY OF TORONTO

Hacked passwords

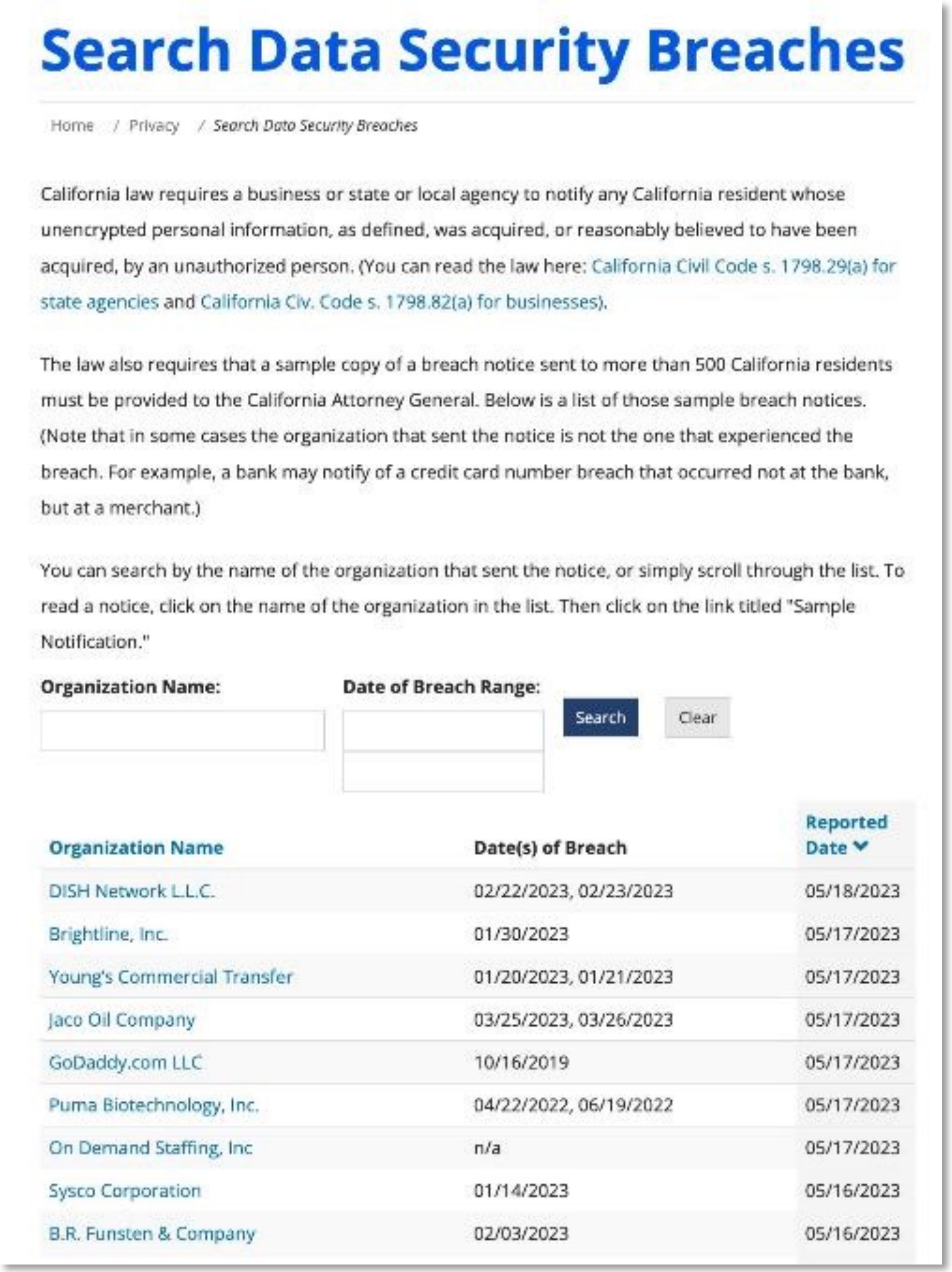
- Go to this website https://github.com/danielmiessler/SecLists
- See examples how threat actors are using stolen passwords

SciNet

Data Security Breaches State of California (USA)

Some of the companies that we use on a daily basis are really bad in securing our information/ passwords

- Go to this website https://oag.ca.gov/privacy/databreach/list
- See a list of all companies that submitted a customer data breach due to stricter disclosure laws



Search Data Security Breaches

Home / Privacy / *Search Data Security Breaches*

California law requires a business or state or local agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (You can read the law here: California Civil Code s. 1798.29(a) for state agencies and California Civ. Code s. 1798.82(a) for businesses).

The law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General. Below is a list of those sample breach notices. (Note that in some cases the organization that sent the notice is not the one that experienced the breach. For example, a bank may notify of a credit card number breach that occurred not at the bank, but at a merchant.)

You can search by the name of the organization that sent the notice, or simply scroll through the list. To read a notice, click on the name of the organization in the list. Then click on the link titled "Sample Notification."

Organization Name:

Date of Breach Range:

Organization Name	Date(s) of Breach	Reported Date
DISH Network L.L.C.	02/22/2023, 02/23/2023	05/18/2023
Brightline, Inc.	01/30/2023	05/17/2023
Young's Commercial Transfer	01/20/2023, 01/21/2023	05/17/2023
Jaco Oil Company	03/25/2023, 03/26/2023	05/17/2023
GoDaddy.com LLC	10/16/2019	05/17/2023
Puma Biotechnology, Inc.	04/22/2022, 06/19/2022	05/17/2023
On Demand Staffing, Inc	n/a	05/17/2023
Sysco Corporation	01/14/2023	05/16/2023
B.R. Funsten & Company	02/03/2023	05/16/2023

UNIVERSITY OF TORONTO

Self-hosting benefits

- Control over your own data/password
- Control over your Operating system/ VM/ dockers environment
- Minimize the risk of unauthorized access and data breaches
- Access to features that are not available on free tier password managers
- Flexible – can be customized for your instance
- Gain knowledge and learn about encryption, backups, and securing your own infrastructure

Potential challenges and considerations

- You are the system administrator
- Backups – need to stay current, encrypted and safe.
- Implementation and environment set up
- Cost of hardware and software (if not using open-source project)
- Responsible for your data, set-up and updates
- Monitor the system for attacks and potential beaches
- Domain name
- Email service

Other drawbacks and concerns

Dependency on the master password: Losing or forgetting the master password may result in permanent data loss

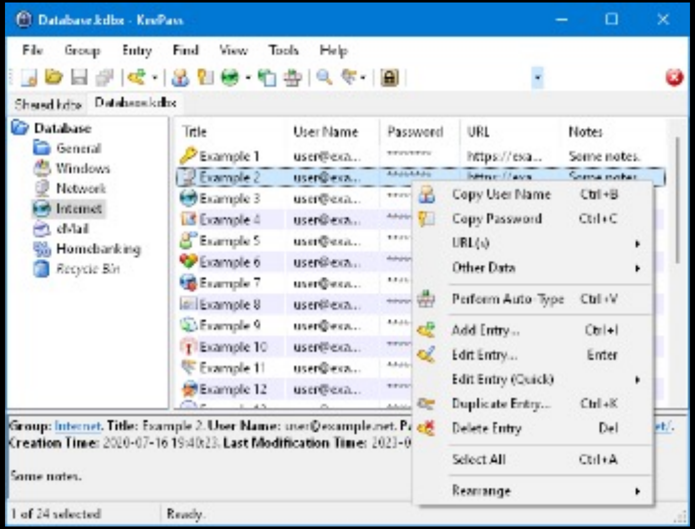
Single point of failure: If the password manager is compromised, all stored passwords may be at risk

Trust in the cloud provider if hosting in cloud

Learning curve: New users may find it challenging to adapt to a password manager initially.

You are responsible for your data

Password managers
Options

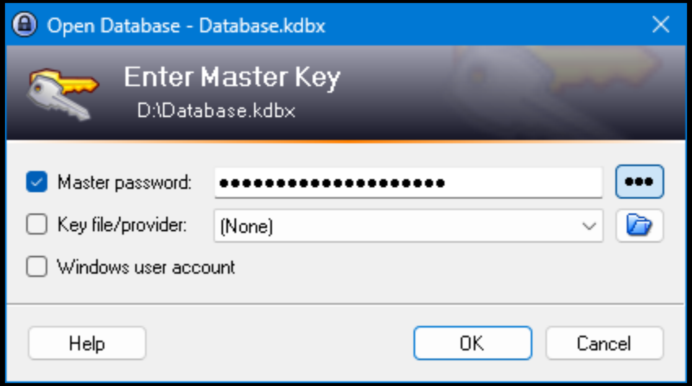


Title	User Name	Password	URL	Notes
Example 1	user@exa...	********	https://exa...	Some notes.
Example 2	user@exa...	********	https://exa...	Some notes.
Example 3	user@exa...	****		
Example 4	user@exa...	****		
Example 5	user@exa...	****		
Example 6	user@exa...	****		
Example 7	user@exa...	****		
Example 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** ... et/.
Creation Time: 2020-07-16 19:40:23. **Last Modification Time:** 2023-0

Some notes.

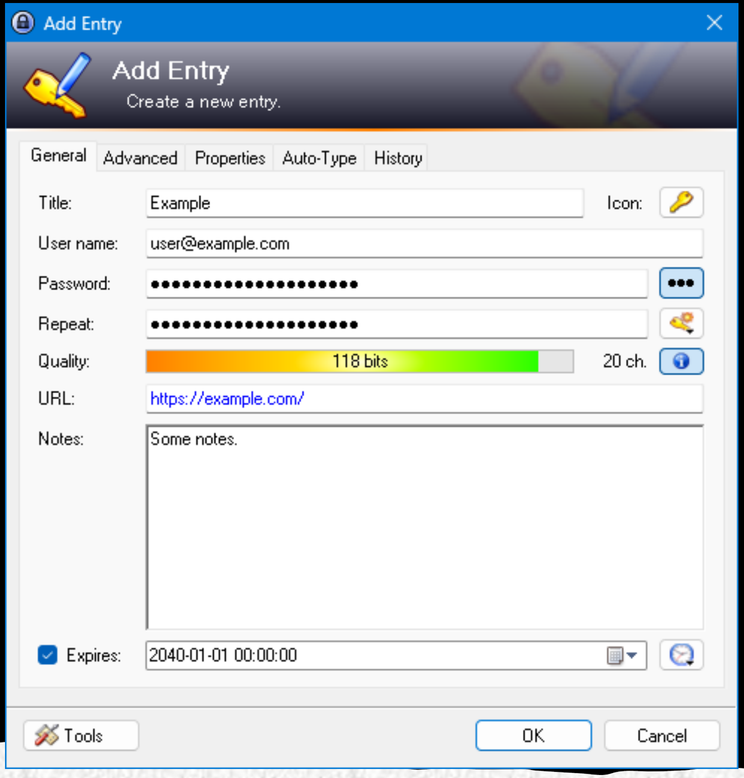
1 of 24 selected Ready.



☑ Master password: ••••••••••••••••••••

☐ Key file/provider: (None)

☐ Windows user account



Title: Example

Icon:

User name: user@example.com

Password: •••••••••••••••••••

Repeat: •••••••••••••••••••

Quality: 118 bits 20 ch.

URL: https://example.com/

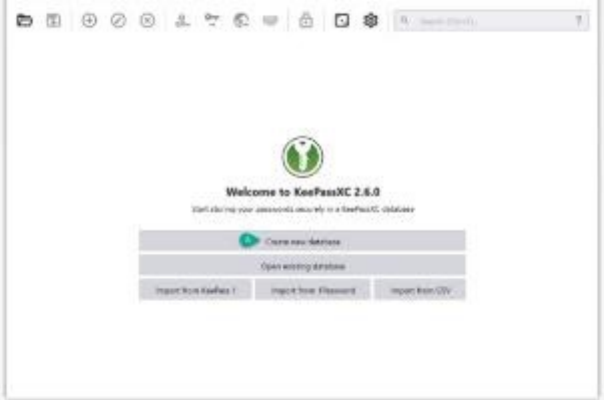
Notes: Some notes.

☑ Expires: 2040-01-01 00:00:00

KeePass

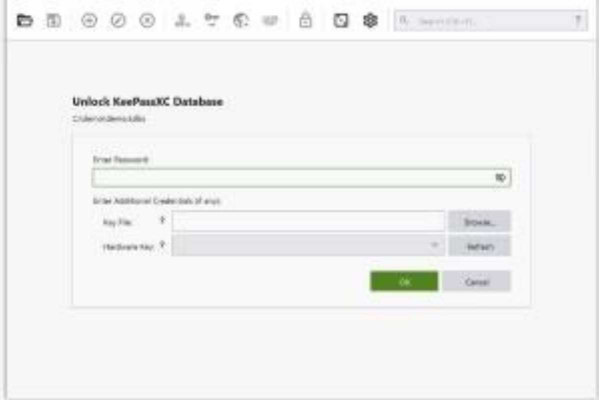
- KeePass been around for 19+ years
- It has limited features and no MFA but it has a key file
- Local storge

UNIVERSITY OF TORONTO SciNet

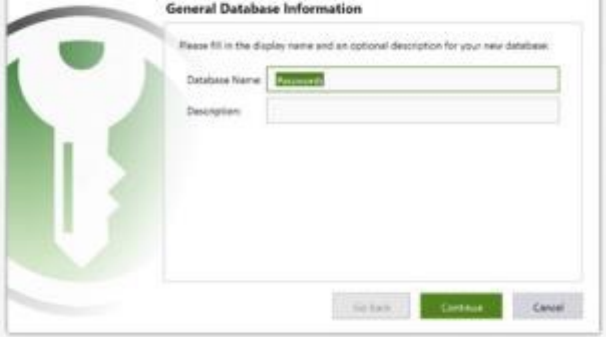

Welcome to KeePassXC 2.6.0

Start storing your passwords securely in a KeePassXC database

Welcome Screen


Unlock KeePassXC Database

Unlock Database

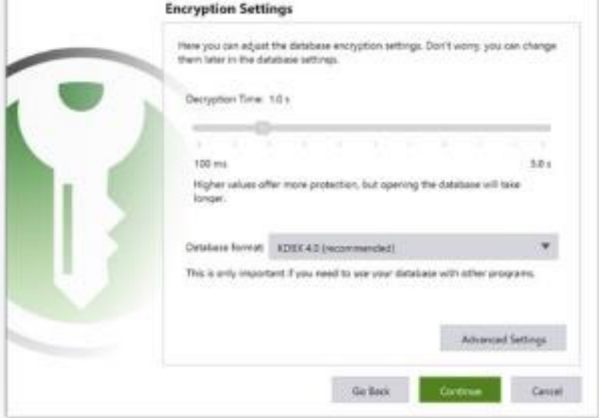

General Database Information

Please fill in the display name and an optional description for your new database:

Database Name: Passwords

Description:

New Database Wizard


Encryption Settings

Here you can adjust the database encryption settings. Don't worry, you can change them later in the database settings.

Decryption Time: 1.0 s

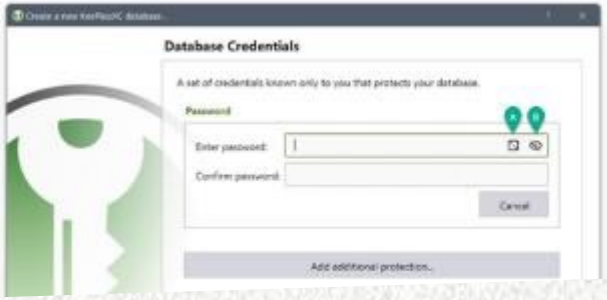
100 ms — 5.0 s

Higher values offer more protection, but opening the database will take longer.

Database format: KDBX 4.0 (recommended)

This is only important if you need to use your database with other programs.

New Database Wizard

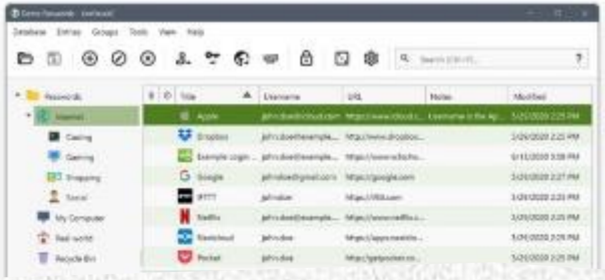

Database Credentials

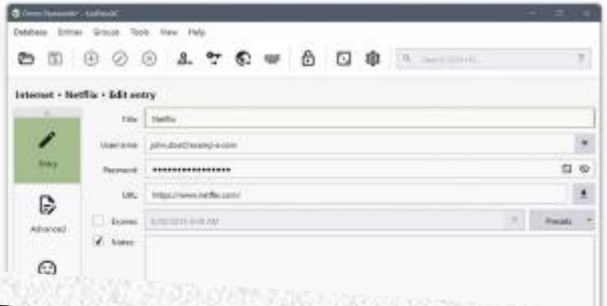
A set of credentials known only to you that protects your database.

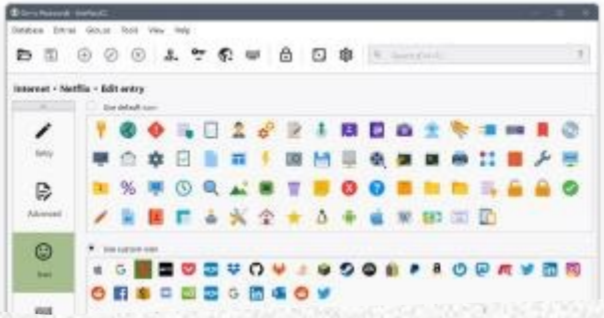
Password

Enter password:

Confirm password:




Internet › Netflix › Edit entry


Internet › Netflix › Edit entry

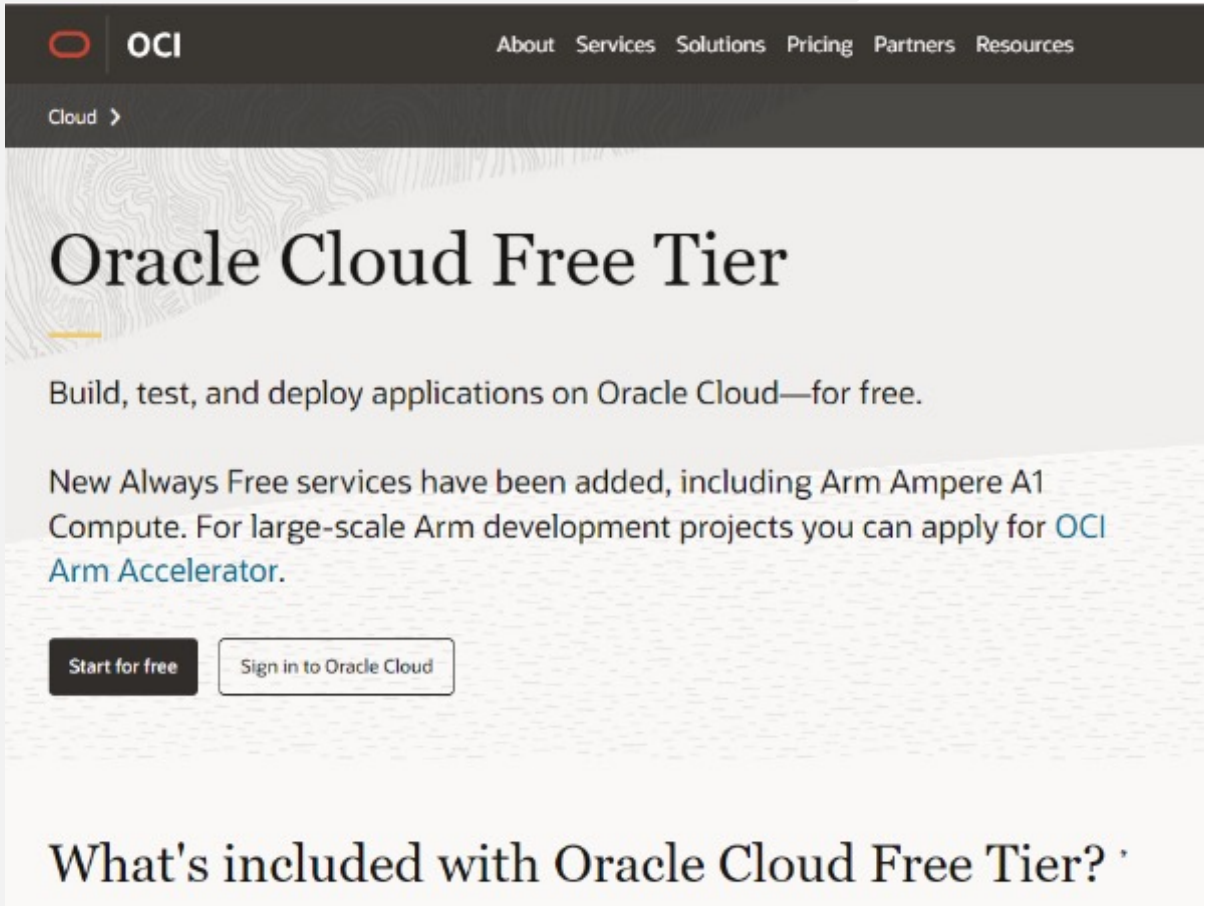
KeePassXC

- KeePassXC multi-platform fork of KeePass
- It has more features vs. KeePass
- Local storge

sync.com Dropbox OneDrive Google Cloud

Cloud storage

- sync.com
- dropbox.com
- onedrive.live.com
- drive.google.com



Oracle Cloud Free Tier

Build, test, and deploy applications on Oracle Cloud—for free.

New Always Free services have been added, including Arm Ampere A1 Compute. For large-scale Arm development projects you can apply for OCI Arm Accelerator.

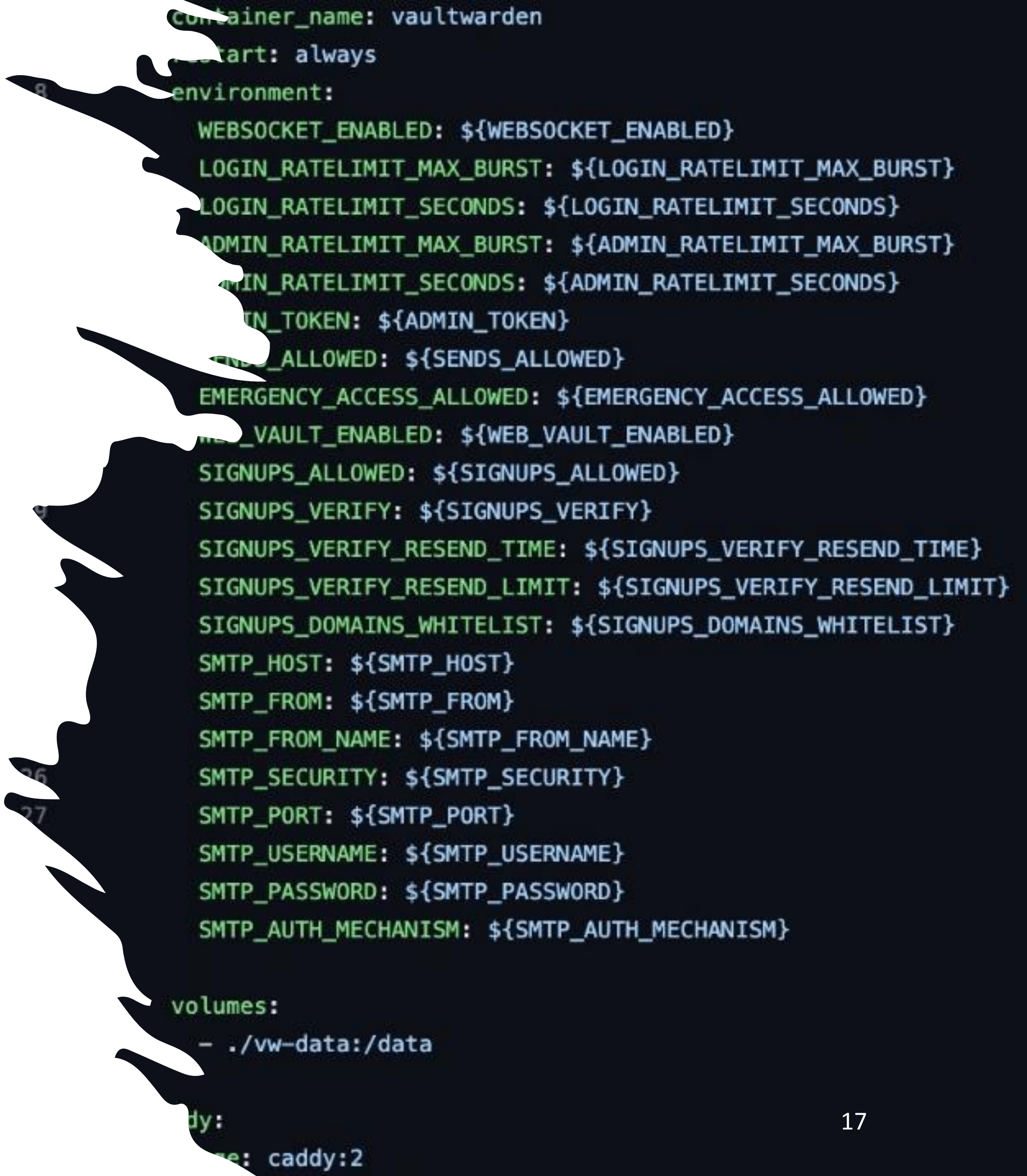
What's included with Oracle Cloud Free Tier?

Oracle Cloud Free Tier

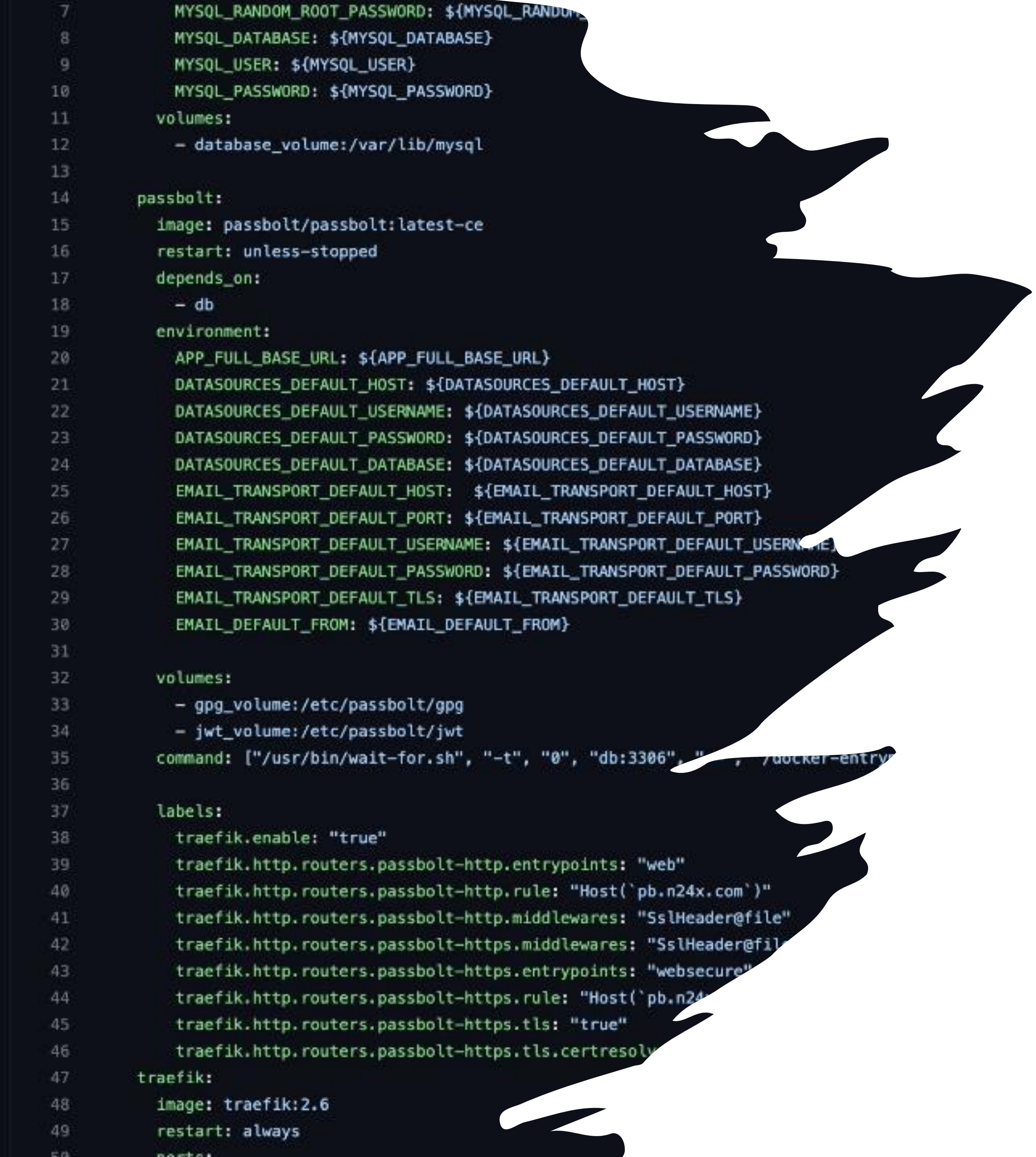
- For more Free Tier providers click here https://github.com/cloudcommunity/Cloud-Free-Tier-Comparison

Vaultwarden docker-compose

- Go here for example implementation https://github.com/n24x/demo-vaultwarden



```
    container_name: vaultwarden
    restart: always
    environment:
      WEBSOCKET_ENABLED: ${WEBSOCKET_ENABLED}
      LOGIN_RATELIMIT_MAX_BURST: ${LOGIN_RATELIMIT_MAX_BURST}
      LOGIN_RATELIMIT_SECONDS: ${LOGIN_RATELIMIT_SECONDS}
      ADMIN_RATELIMIT_MAX_BURST: ${ADMIN_RATELIMIT_MAX_BURST}
      ADMIN_RATELIMIT_SECONDS: ${ADMIN_RATELIMIT_SECONDS}
      ADMIN_TOKEN: ${ADMIN_TOKEN}
      SENDS_ALLOWED: ${SENDS_ALLOWED}
      EMERGENCY_ACCESS_ALLOWED: ${EMERGENCY_ACCESS_ALLOWED}
      WEB_VAULT_ENABLED: ${WEB_VAULT_ENABLED}
      SIGNUPS_ALLOWED: ${SIGNUPS_ALLOWED}
      SIGNUPS_VERIFY: ${SIGNUPS_VERIFY}
      SIGNUPS_VERIFY_RESEND_TIME: ${SIGNUPS_VERIFY_RESEND_TIME}
      SIGNUPS_VERIFY_RESEND_LIMIT: ${SIGNUPS_VERIFY_RESEND_LIMIT}
      SIGNUPS_DOMAINS_WHITELIST: ${SIGNUPS_DOMAINS_WHITELIST}
      SMTP_HOST: ${SMTP_HOST}
      SMTP_FROM: ${SMTP_FROM}
      SMTP_FROM_NAME: ${SMTP_FROM_NAME}
      SMTP_SECURITY: ${SMTP_SECURITY}
      SMTP_PORT: ${SMTP_PORT}
      SMTP_USERNAME: ${SMTP_USERNAME}
      SMTP_PASSWORD: ${SMTP_PASSWORD}
      SMTP_AUTH_MECHANISM: ${SMTP_AUTH_MECHANISM}

    volumes:
      - ./vw-data:/data

  caddy:
    image: caddy:2
```

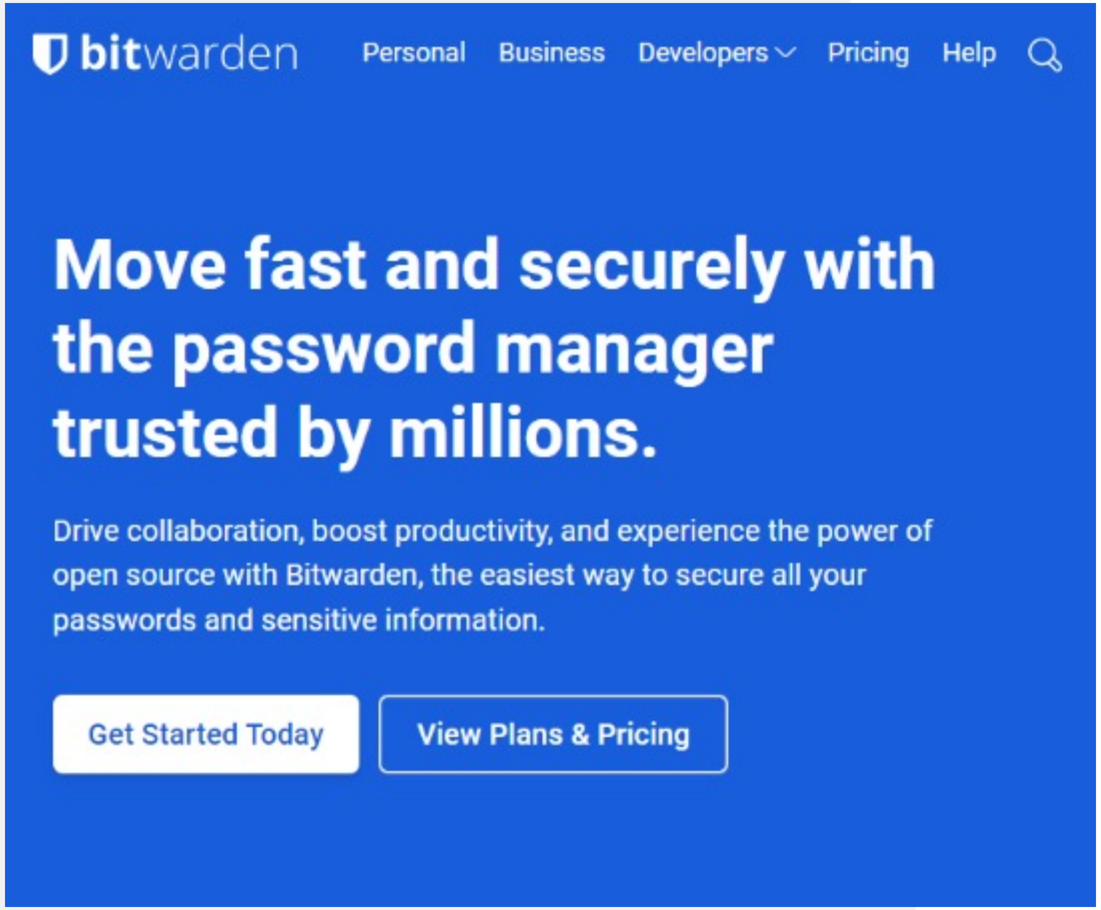


```
        MYSQL_RANDOM_ROOT_PASSWORD: ${MYSQL_RANDO
        MYSQL_DATABASE: ${MYSQL_DATABASE}
        MYSQL_USER: ${MYSQL_USER}
        MYSQL_PASSWORD: ${MYSQL_PASSWORD}
      volumes:
        - database_volume:/var/lib/mysql

    passbolt:
      image: passbolt/passbolt:latest-ce
      restart: unless-stopped
      depends_on:
        - db
      environment:
        APP_FULL_BASE_URL: ${APP_FULL_BASE_URL}
        DATASOURCES_DEFAULT_HOST: ${DATASOURCES_DEFAULT_HOST}
        DATASOURCES_DEFAULT_USERNAME: ${DATASOURCES_DEFAULT_USERNAME}
        DATASOURCES_DEFAULT_PASSWORD: ${DATASOURCES_DEFAULT_PASSWORD}
        DATASOURCES_DEFAULT_DATABASE: ${DATASOURCES_DEFAULT_DATABASE}
        EMAIL_TRANSPORT_DEFAULT_HOST:  ${EMAIL_TRANSPORT_DEFAULT_HOST}
        EMAIL_TRANSPORT_DEFAULT_PORT: ${EMAIL_TRANSPORT_DEFAULT_PORT}
        EMAIL_TRANSPORT_DEFAULT_USERNAME: ${EMAIL_TRANSPORT_DEFAULT_USERNAME}
        EMAIL_TRANSPORT_DEFAULT_PASSWORD: ${EMAIL_TRANSPORT_DEFAULT_PASSWORD}
        EMAIL_TRANSPORT_DEFAULT_TLS: ${EMAIL_TRANSPORT_DEFAULT_TLS}
        EMAIL_DEFAULT_FROM: ${EMAIL_DEFAULT_FROM}

      volumes:
        - gpg_volume:/etc/passbolt/gpg
        - jwt_volume:/etc/passbolt/jwt
      command: ["/usr/bin/wait-for.sh", "-t", "0", "db:3306", "--", "/docker-entry

      labels:
        traefik.enable: "true"
        traefik.http.routers.passbolt-http.entrypoints: "web"
        traefik.http.routers.passbolt-http.rule: "Host(`pb.n24x.com`)"
        traefik.http.routers.passbolt-http.middlewares: "SslHeader@file"
        traefik.http.routers.passbolt-https.middlewares: "SslHeader@fil
        traefik.http.routers.passbolt-https.entrypoints: "websecure"
        traefik.http.routers.passbolt-https.rule: "Host(`pb.n24
        traefik.http.routers.passbolt-https.tls: "true"
        traefik.http.routers.passbolt-https.tls.certresolv
    traefik:
      image: traefik:2.6
      restart: always
      ports:
```

Passbolt docker-compose

- Go here for example implementation https://github.com/n24x/demo_setup_passbolt
- Learn more about this password manager here https://help.passbolt.com/

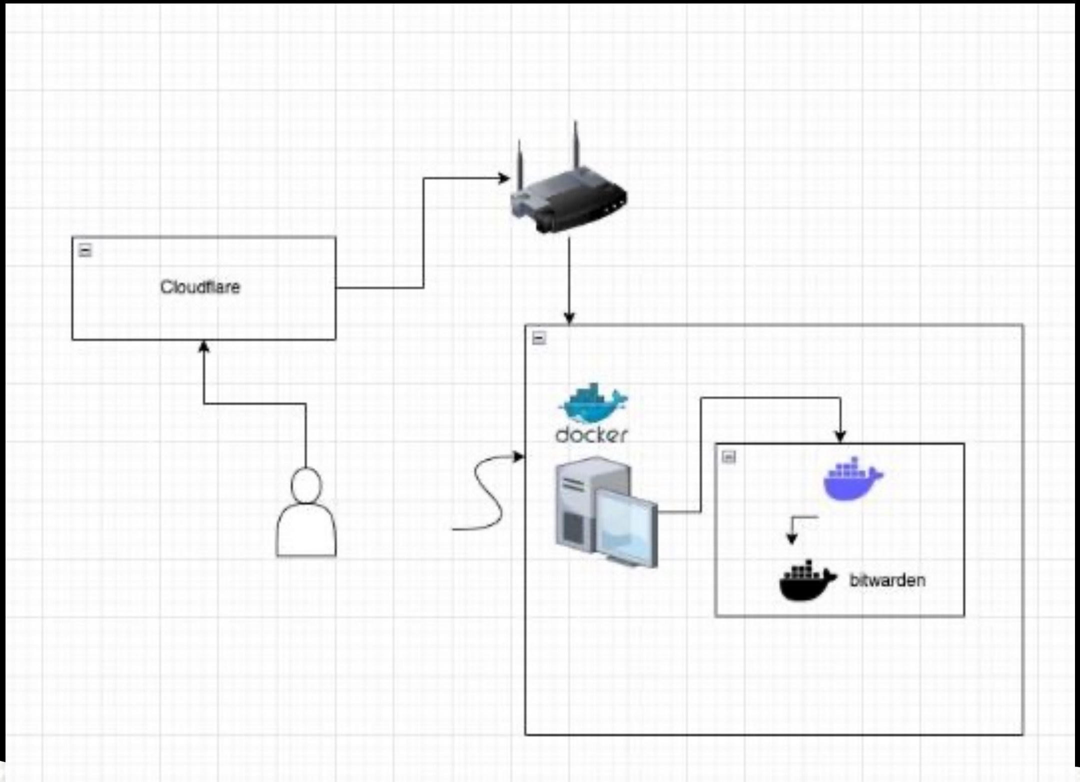
Bitwarden



Move fast and securely with the password manager trusted by millions.

Drive collaboration, boost productivity, and experience the power of open source with Bitwarden, the easiest way to secure all your passwords and sensitive information.

- Go here to implement this option https://bitwarden.com/help/install-on-premise-linux/
- Learn more about this password manager here https://bitwarden.com/help/



Cloudflare Tunnel

- Complex implementation
- You need to trust Cloudflare – this is a proxy and Cloudflare can see all your traffic

1Password DASHLANE bitwarden RoboForm

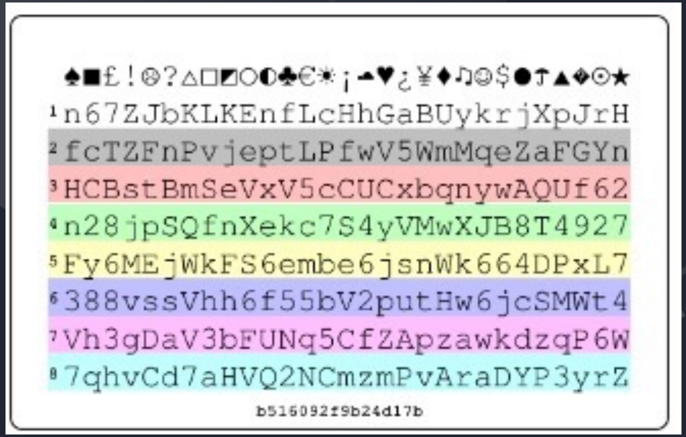
Paid Services

- https://1password.com/
- https://www.dashlane.com/
- https://bitwarden.com/
- https://www.roboform.com/

UNIVERSITY OF TORONTO

Tips for creating a master password

- **Use a made-up word** – that is not in a dictionary, make it up, Google a fake word generator. i.e. egalezone , slowaturaz, firebozaga , learngos
- **Make it memorable to you** – use a phrase from a book or a song know and love
- Or **create your own password card** – go here https://www.passwordcard.org/en
- **Keep it simple** it doesn't need to be complicated



```
 ♠■£!☹?△□◩○◐♣€☀¡☁♥¿¥♦♫☺$●↑▲◆⊙★
1n67ZJbKLKEnfLcHhGaBUykrjXpJrH
2fcTZFnPvjeptLPfwV5WmMqeZaFGYn
3HCBstBmSeVxV5cCUCxbqnywAQUf62
4n28jpSQfnXekc7S4yVMwXJB8T4927
5Fy6MEjWkFS6embe6jsnWk664DPxL7
6388vssVhh6f55bV2putHw6jcSMWt4
7Vh3gDaV3bFUNq5CfZApzawkdzqP6W
87qhvCd7aHVQ2NCmzmPvAraDYP3yrZ
           b516092f9b24d17b
```

SciNet

Once you have your master password…

- Use MFA – i.e. google authenticator, Microsoft Authenticator, or any other similar app
- Don’t store your MFA keys in your password manager – keep them separate
- Use a hardware key (i.e. YubiKey) but remember you should have at lease 2: one primary and one as a backup
- Or use the Duo app

Thank you!

Any questions?