Willow Valley Computer Club

Member of apcug An International Association of Technology & Computer User Groups

Password Managers

What are they?

Why would I want to use one?

Al Williams

March 2, 2023

12345

1234567

w12345

rockyou 14,344,392 passwords

12345

1234567

w12345

rockyou a few 18 character passwords

123456789987654321

Websites store our password in encrypted form. They use the password to verify that it is us logging into the account.

MD5 encryption

Password: target2!

MD5: fcb83491ade142ed34ff820ff86c4d08

3 minutes and 33 seconds to brute force

Password: Target2!

MD5: 1729862c51976bfc1bfcdbdb62541a96

41 hours, 58 minutes and 38 seconds to brute force.

If we reuse a password for more than one account and one of those accounts is exposed in a data breach

The hacker will use our email address and the exposed password and try to log into other accounts

When the hacker finds an account that reuses the password, the hacker controls the account

HaveIBeenPwned.com

Enter your email address.

The website will display all breached accounts associated with that email address

The website will also say if the account’s password was exposed.

Password Lists or Reuse across accounts

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	Instantly
9	Instantly	Instantly	Instantly	Instantly	Instantly
10	Instantly	Instantly	Instantly	Instantly	Instantly
11	Instantly	Instantly	Instantly	Instantly	Instantly
12	Instantly	Instantly	Instantly	Instantly	Instantly
13	Instantly	Instantly	Instantly	Instantly	Instantly
14	Instantly	Instantly	Instantly	Instantly	Instantly
15	Instantly	Instantly	Instantly	Instantly	Instantly
16	Instantly	Instantly	Instantly	Instantly	Instantly
17	Instantly	Instantly	Instantly	Instantly	Instantly
18	Instantly	Instantly	Instantly	Instantly	Instantly

Source: hivesystems.io

We need to use a unique password for each account to ensure that if a password is leaked, loss is limited to that account.

Cybersecurity experts urge us to use long and complex passwords because it takes a long time to crack those passwords.

Lower case
Upper case
Number
Symbol

GPU – Graphical Processing Unit

Gaming
Video Editing
Content Creation
Machine Learning
Password cracking

MD5

GPU:
RTX 3090

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	3 secs
7	Instantly	Instantly	15 secs	51 secs	4 mins
8	Instantly	3 secs	13 mins	52 mins	5 hours
9	Instantly	1 mins	11 hours	2 days	2 weeks
10	Instantly	34 mins	3 weeks	5 months	3 years
11	1 sec	15 hours	3 years	24 years	300 years
12	14 secs	2 weeks	200 years	1k years	20k years
13	2 mins	1 year	9k years	91k years	2m years
14	24 mins	29 years	483k years	6m years	118m years
15	4 hours	800 years	25m years	251m y	9bn years
16	2 days	20k years	1bn years	22bn y	697bn years
17	2 weeks	518k years	68bn years	1tn years	54tn years
18	5 months	13m years	4tn years	84tn years	4qd years

Source:
hivesystems.io

Password managers use PBKDF2-SHA256 encryption

PBKDF2-SHA256

GPU:
RTX 3090

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	2 secs	4 secs	4 secs
5	Instantly	3 secs	2 mins	4 mins	12 mins
6	Instantly	1 min	1 hour	4 hours	15 hours
7	3 secs	35 mins	3 days	2 weeks	2 months
8	26 secs	15 hours	5 months	2 years	10 years
9	4 mins	2 weeks	23 years	100 years	800 years
10	44 mins	1 year	1k years	7k years	61k years
11	7 hours	31 years	63k years	435k years	5m years
12	3 days	800 years	3m years	27m years	363m years
13	1 month	21k years	170m years	2bn years	28bn years
14	10 months	539k years	9bn years	104bn years	2tn years
15	8 years	14m years	460bn years	6tn years	166tn years
16	84 years	365m years	24tn years	399 tn years	13 qdn years
17	800 years	9bn years	1qdn years	25 qdn years	983 qdn years
18	8k years	246bn years	65 qdn years	2 qntn yrs	76qntn years

Source:
hivesystems.io

The graph shows that a 9 character password with upper and lower case letters, a number and a symbol would take 800 years to crack.

Why is that entry colored orange?

Because hackers can use multiple GPUs to crack a password – also, GPUs continue to get faster

Also, that 9 character password might be in a password list

Choosing a master password for your password manager and passwords for websites

- Federal agencies recommend 12 character passwords
- hivesystems.io recommends complex passwords with 16 characters or more
- To avoid using an existing password in a password list, use complex passwords with 19 characters or more

MD5

GPU:
RTX 3090

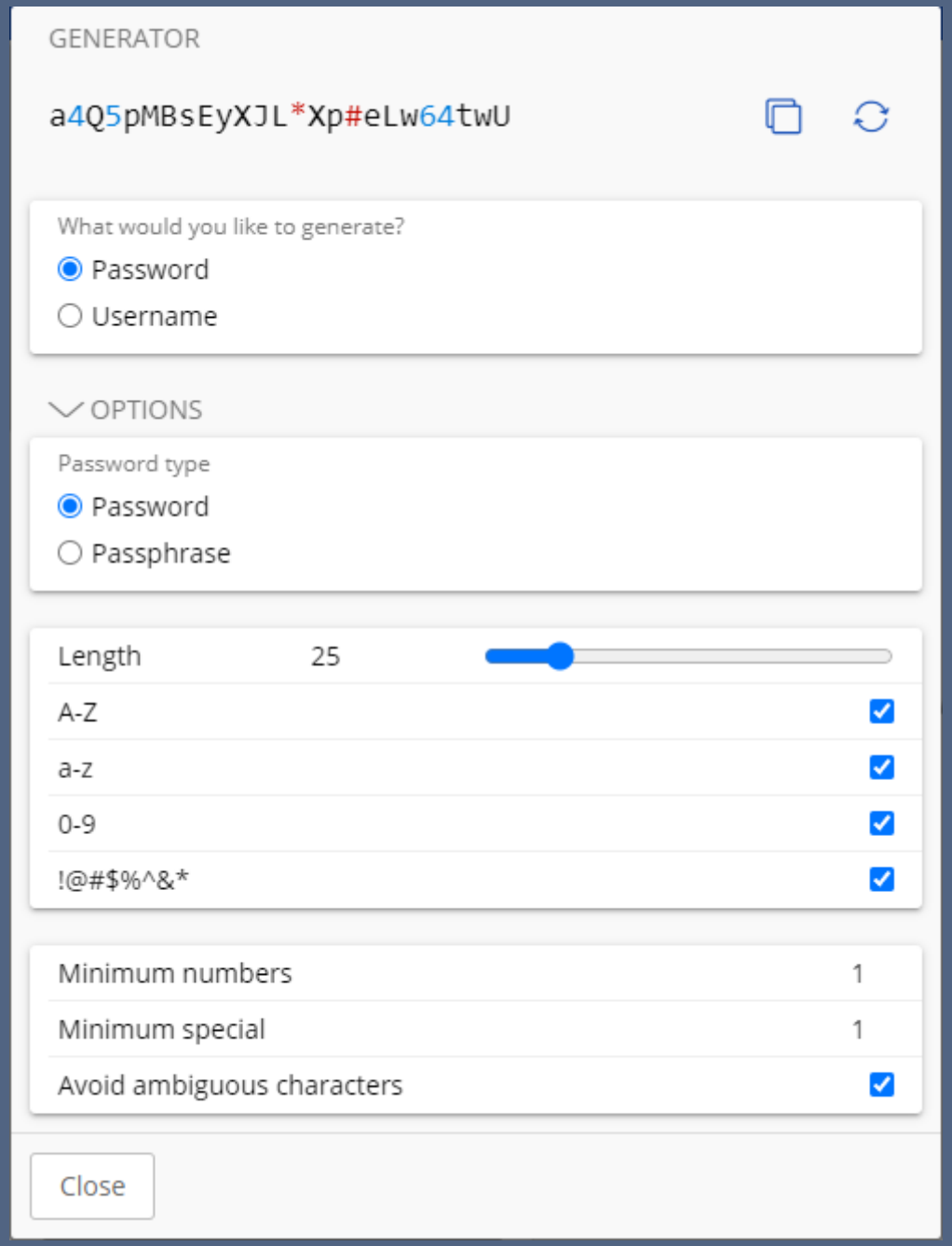
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	3 secs
7	Instantly	Instantly	15 secs	51 secs	4 mins
8	Instantly	3 secs	13 mins	52 mins	5 hours
9	Instantly	1 mins	11 hours	2 days	2 weeks
10	Instantly	34 mins	3 weeks	5 months	3 years
11	1 sec	15 hours	3 years	24 years	300 years
12	14 secs	2 weeks	200 years	1k years	20k years
13	2 mins	1 year	9k years	91k years	2m years
14	24 mins	29 years	483k years	6m years	118m years
15	4 hours	800 years	25m years	251m y	9bn years
16	2 days	20k years	1bn years	22bn y	697bn years
17	2 weeks	518k years	68bn years	1tn years	54tn years
18	5 months	13m years	4tn years	84tn years	4qd years

Source:
hivesystems.io

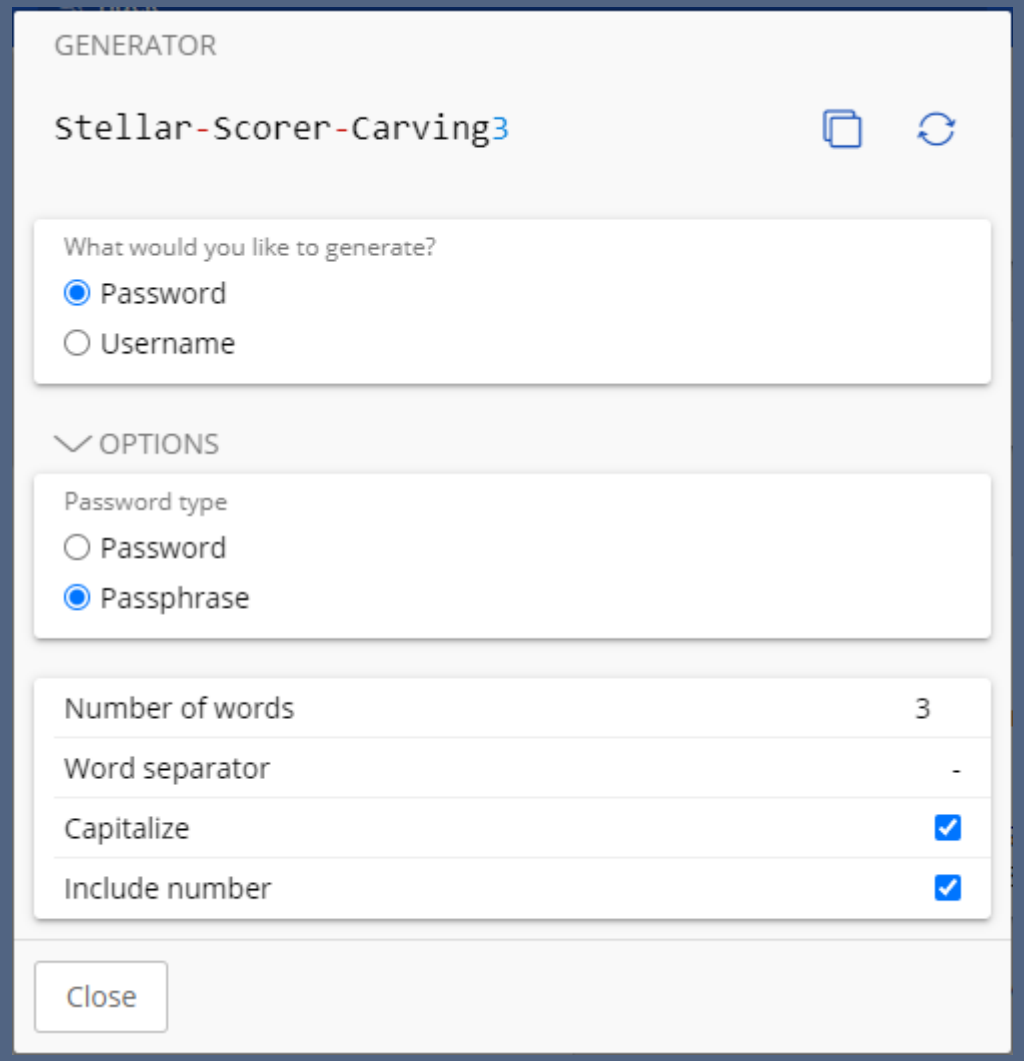
How do you create long, random, and complex passwords or passphrases for each account?

- Roll dice for words
- Use a password or passphrase generator

Bitwarden Password Manager
The password generator



Bitwarden Password Manager
The passphrase generator



What else can a password manager do?

- It can store your passwords and passphrases
- The password manager lets you search for accounts, you don’t have to remember passwords or passphrases
- You don’t have to look through sheets of paper to find them

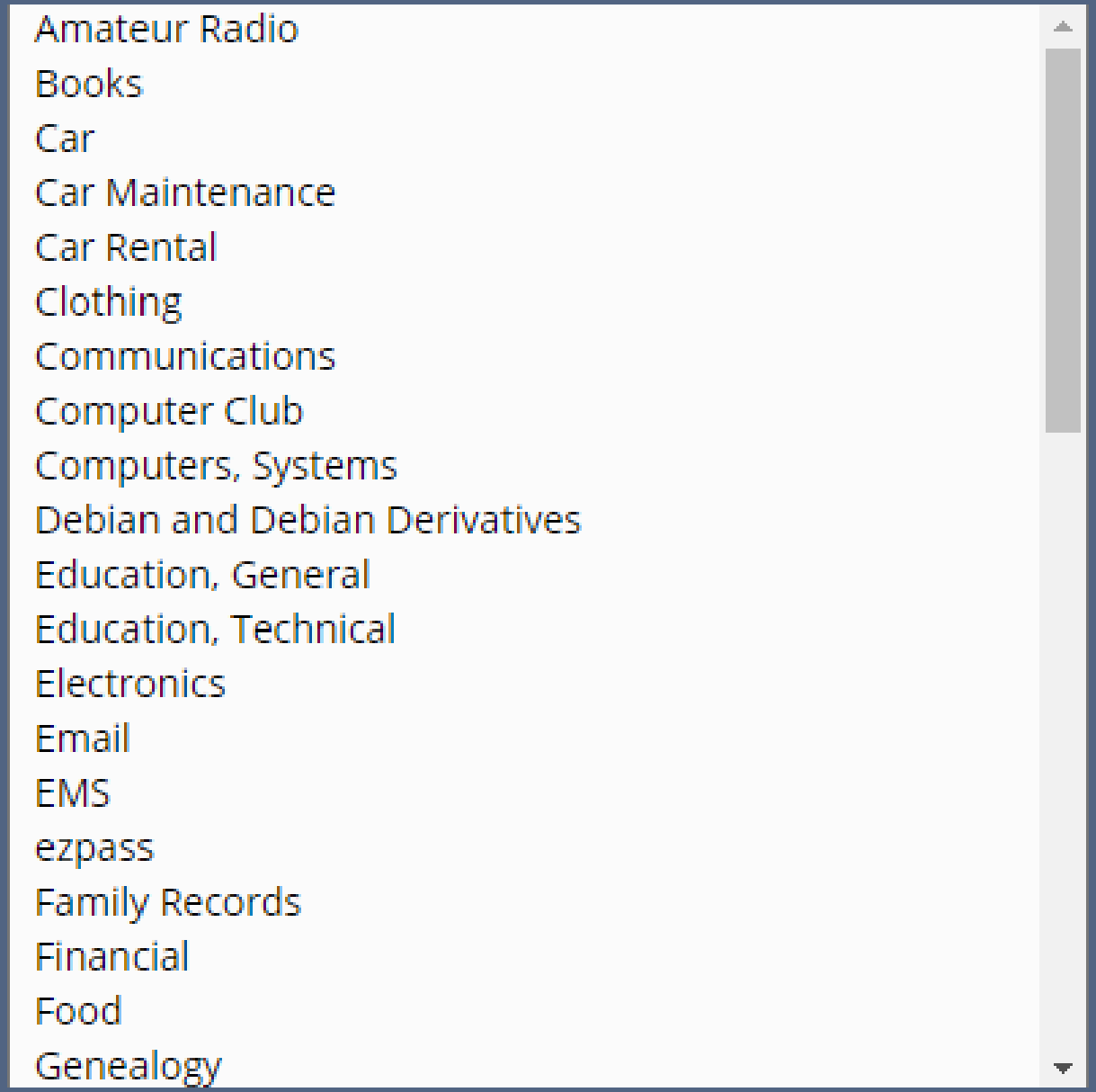
What else can a password manager do?

You can organize your accounts using folders

How many accounts and secure notes do you have?

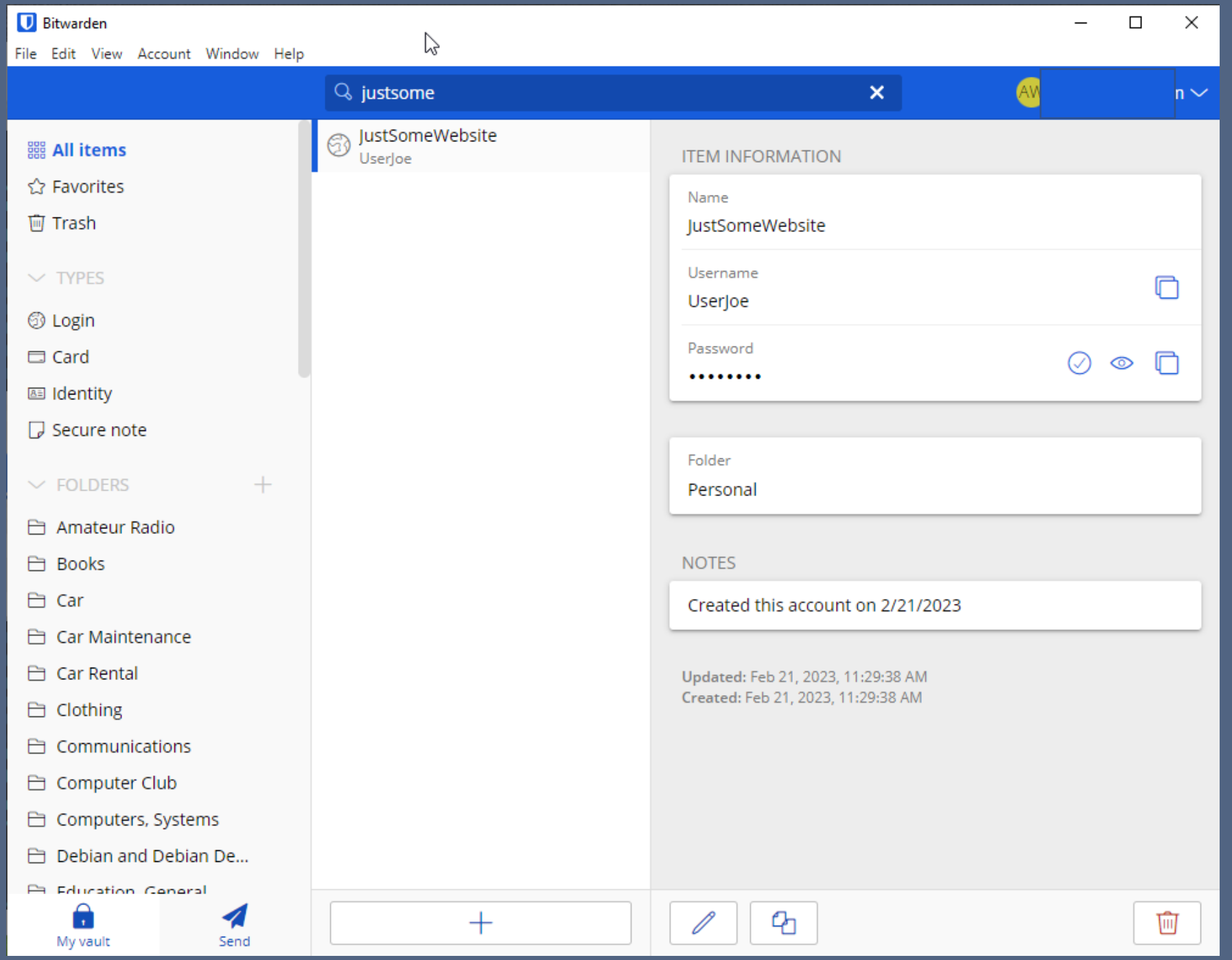
I have 466

I have 51 folders



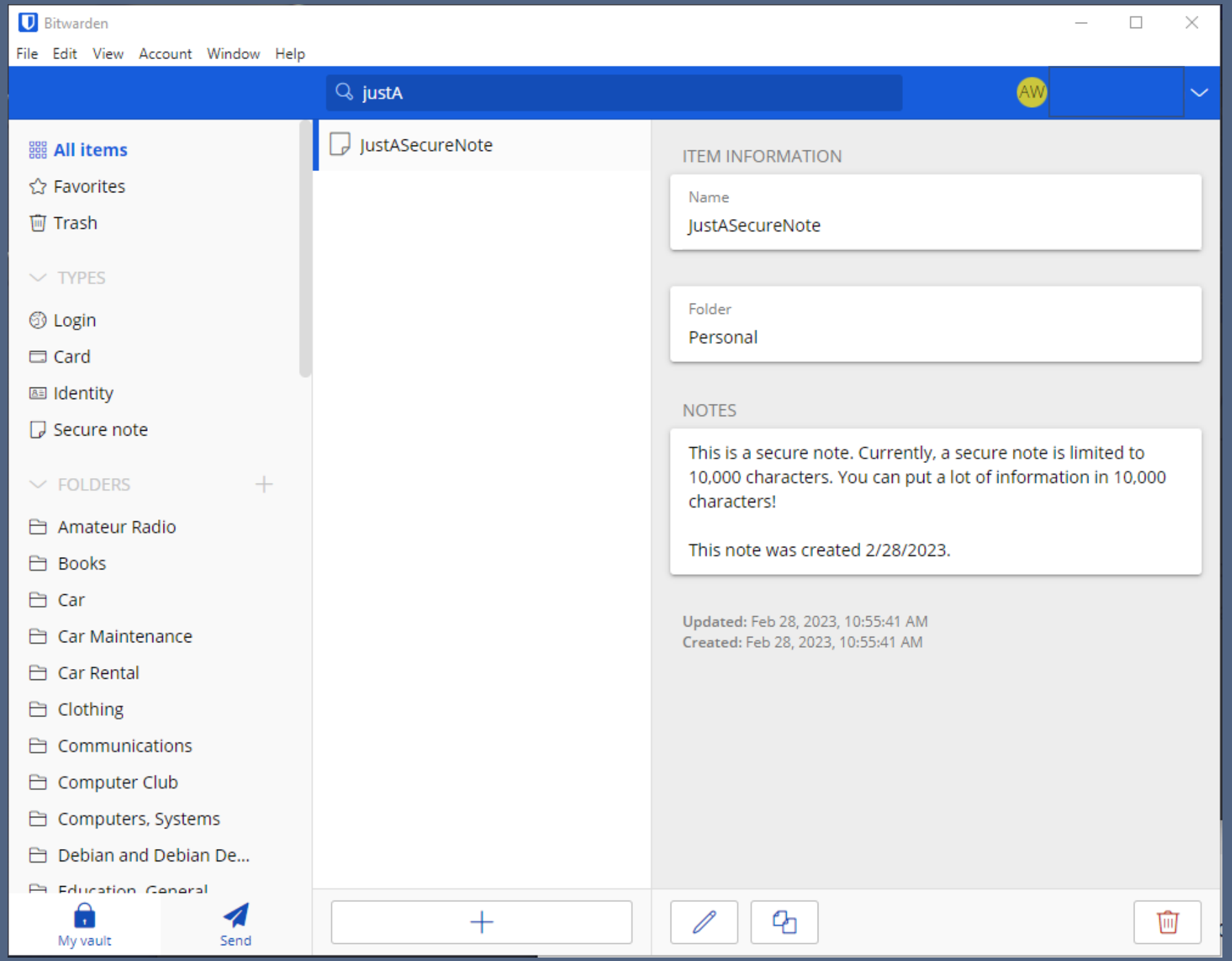
A Bitwarden Vault

Demo Account Displayed



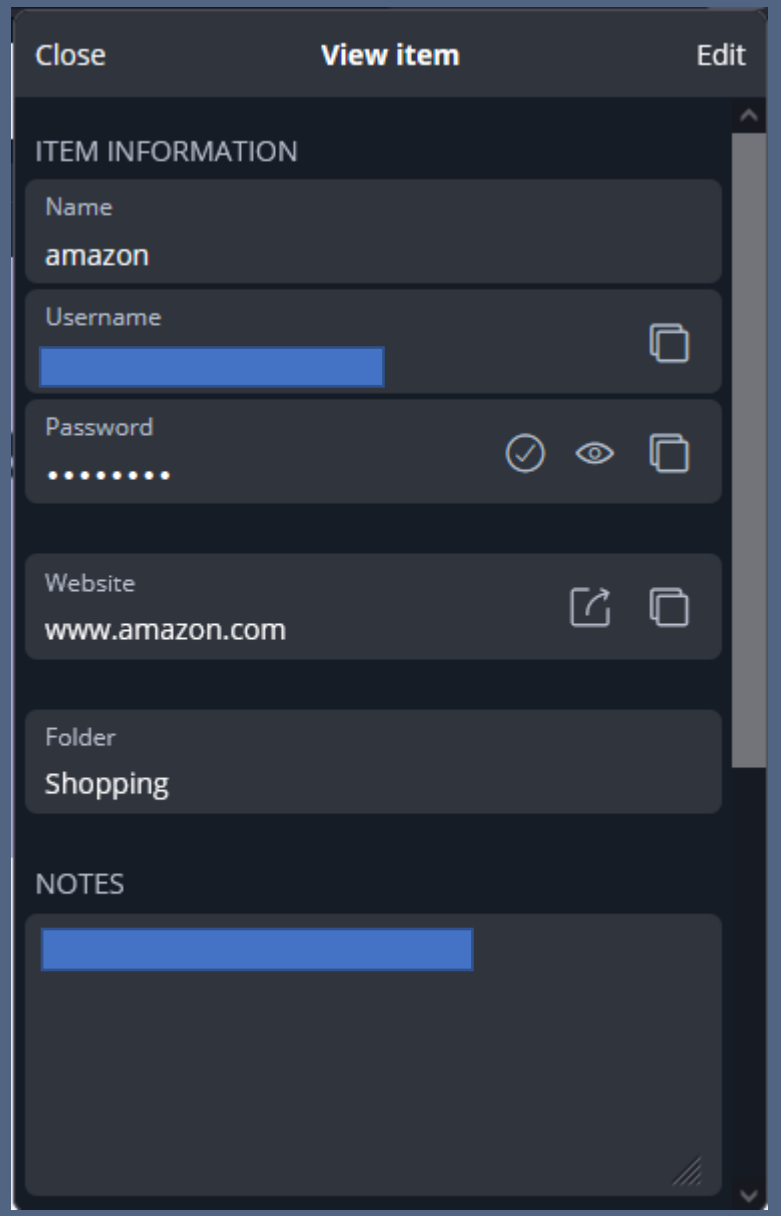
A Bitwarden Vault

Demo Secure Note Displayed



Bitwarden
Browser Extension

Account Login
Displayed



What can a password manager do?

- Create passwords or passphrases
- Store your username and password for each account – and notes about that account
- Store secure notes

What else can a password manager do?

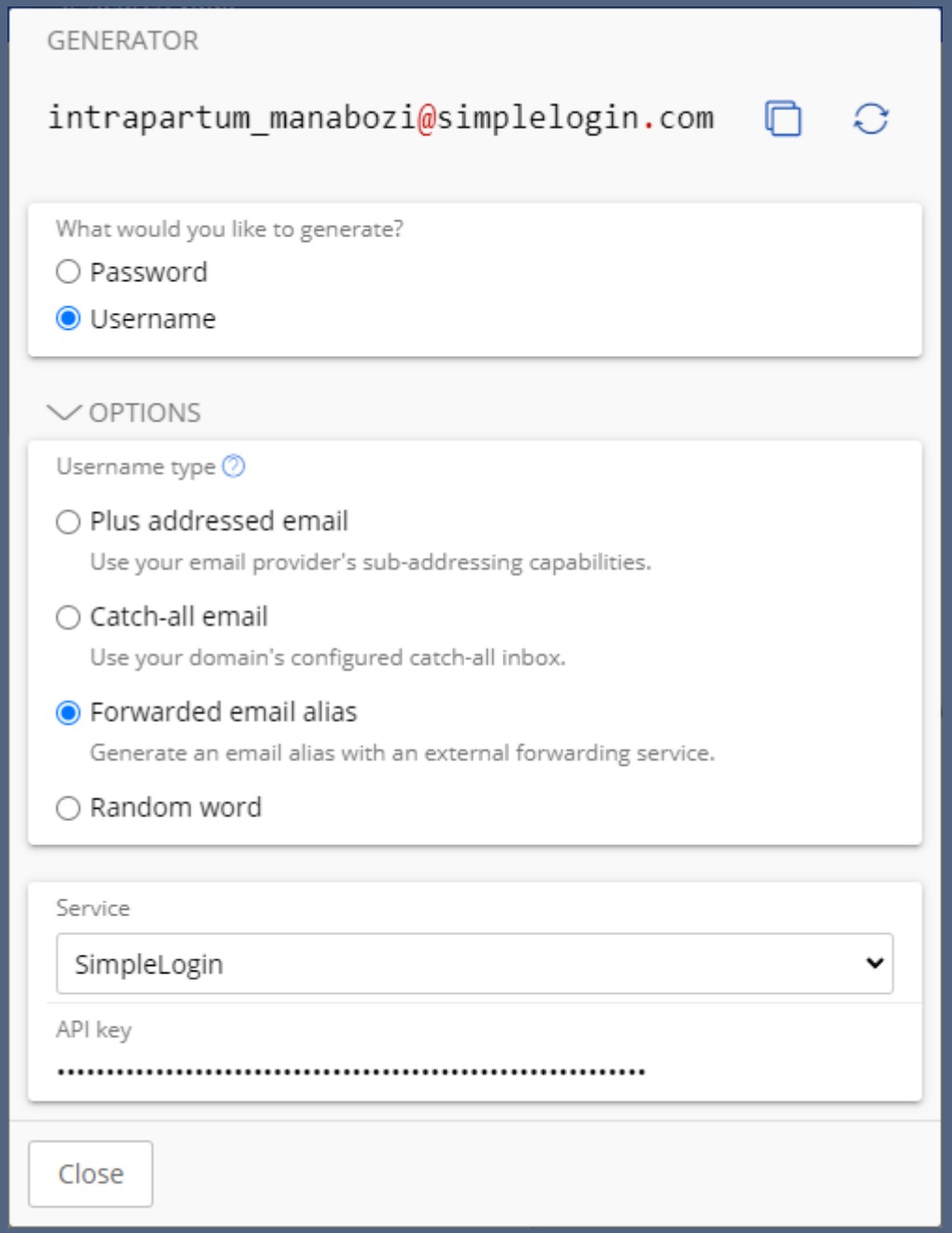
It can create email aliases

Our email addresses identify who we are

Using a different email alias on each account makes it difficult for a hacker who hacks one of our accounts to find our other accounts.

Bitwarden Password Manager
The email alias generator

A SimpleLogin alias



What else can a password manager do?

- It can autofill login pages
- It allows copying and pasting of usernames and passwords

Tracking passwords using paper

- Do you cross out old passwords?
- Can you find the passwords you need?
- Can you type the long, random, and complex passwords with the recommended 16, or more, characters?

Top ranked password managers

Cloud storage

Bitwarden*

1Password

Local storage

KeePassXC**

* Computer Club recommended - because it is open source

** KeePassXC is for technical users

Password managers – Cons – and responses

If the Internet is down, you can't access passwords

You won't need them – but can export your passwords

If you don't create recovery codes, you could lock yourself out

Create recovery codes and store in safe place

If a hacker has your master password, he has all your passwords

Use two-factor authentication to prevent hacker access

What about the LastPass data breach?

If you used a strong master password, your data is safe

LastPass lost control of access to user's data vaults. The vaults were copied by someone

Those individuals can now try to crack user's master passwords, using the copy, whenever they wish

Why move from LastPass? LastPass did not keep up with current best practices for encryption

Bitwarden training

Bitwarden 101
Jay Shah
Thursday, June 8 – 1:30 to 2:30pm
Cultural Center Education Room

Bitwarden 102
Jay Shah
Wednesday, June 28 – 1:30 to 2:30pm
Cultural Center Education Room

A handout

Questions?

MD5

GPU:
RTX 3090

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	3 secs
7	Instantly	Instantly	15 secs	51 secs	4 mins
8	Instantly	3 secs	13 mins	52 mins	5 hours
9	Instantly	1 mins	11 hours	2 days	2 weeks
10	Instantly	34 mins	3 weeks	5 months	3 years
11	1 sec	15 hours	3 years	24 years	300 years
12	14 secs	2 weeks	200 years	1k years	20k years
13	2 mins	1 year	9k years	91k years	2m years
14	24 mins	29 years	483k years	6m years	118m years
15	4 hours	800 years	25m years	251m y	9bn years
16	2 days	20k years	1bn years	22bn y	697bn years
17	2 weeks	518k years	68bn years	1tn years	54tn years
18	5 months	13m years	4tn years	84tn years	4qd years

Source:
hivesystems.io

bcrypt

GPU:
RTX 3090

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	5 secs	1 min	3 mins	1 min
5	1 sec	2 mins	1 hour	3 hours	8 hours
6	10 secs	53 mins	2 days	7 days	4 weeks
7	2 min	1 week	4 months	1 year	5 years
8	17 min	11 months	18 years	72 years	400 years
9	3 hours	2 years	900 years	4k years	31k years
10	1 day	46 years	47k years	275k years	2m years
11	2 weeks	1k years	2m years	17m years	185m years
12	4 months	31k years	128m years	1bn years	14bn years
13	3 years	813k years	180m years	66 bn years	1tn years
14	33 years	21m years	346bn years	4tn years	84tn years
15	300 years	550m years	18tn years	252tn years	6qdn years
16	3k years	14bn years	937tn years	6qdn years	500qdn years
17	33k years	372bn years	49qdn years	969qdn years	39qntn years
18	328k years	10tn years	3qntn years	60qntn years	3 sxtn years

Source:
hivesystems.io