CyberSec
Passwords and Password Managers

Tobias Sattler
tobiassattler.com | cybersec.help

“Open sesame”

Ali Baba and the Forty Thieves

History of Passwords

With the magic word “Open sesame”, Ali Baba was able to gain access to the thieves' cave and claim its treasures for himself.

The concept of passwords goes back a long way. The ancient Roman sentries used watchwords to challenge those wishing to enter an area. Over the centuries, the usage evolved but is still used in the military.

Today, you commonly use usernames and passwords during a login process that controls access to protected systems.

Commonly used Passwords

Based on a study in 2021, the most commonly used passwords worldwide are way too simple.

Top 20 from 200

1	123456 *(used 103M times)*	**11**	qwerty123
2	123456789	**12**	000000
3	12345	**13**	1q2w3e
4	qwerty	**14**	aa12345678
5	password	**15**	abc123
6	12345678	**16**	password1
7	111111	**17**	1234
8	123123	**18**	qwertyuiop
9	1234567890	**19**	123321
10	1234567	**20**	password123 *(used 4.7M times)*

All of those were used Million times and needed less than 2 seconds to be cracked.

Reference: NordPass, (2021)

“Open sesame” was too easy, too

As we know, it wasn't a very complex password and, therefore, easy to guess—especially in modern times. So, how could a strong password look like to protect your devices or accounts? There are some simple rules you should follow to set a good one.

1. **Easy to remember:** There are no limits to your creativity when choosing a password. One memorizes a sentence and uses only the 1st letter (or only the second or last) of each word.

2. **The longer, the better:** A good password should be at least eight characters long. However, a good guideline is 20 characters.

3. **All available characters:** Password can usually consist of upper and lower case letters, numbers, and special characters.

4. **Not in dictionaries:** Not suitable as passwords are names of family members, the pet, the best friend, the favorite star, dates of birth, and so on.

5. **Do not be predictable:** Adding simple digits at the end of the password or one of the usual special characters $! ? # at the beginning or end of an otherwise simple password is not recommended.

6. **Password Managers:** Make use of it to manage your different passwords well.

How to improve your Passwords easily

With those 3 options, you can quickly improve your passwords by thinking in a passphrase.

1. Memorize a sentence and use only the 1st letter of each word (or only the second or last). Afterward, change possibly still certain letters into numbers or special characters.

2. Use a whole sentence as a password or string together different words connected by special characters.

3. Another option is randomly choosing 5-6 words from the dictionary and separating them with a space.

This results in a password that is easy to remember, easy to type, and difficult for attackers to crack.

Convert weak Password to a strong one

With these 7 steps, you can create a strong password:

1. Use, e.g., the phrase “Open sesame”.
2. Rephrase it to “Oh dear sesame, please open up”.
3. Transform the word “open” to “OPEN”.
4. Change the uppercase letter “O” to “0” (zero).
5. Replace the whitespaces with hyphens (-) and underscores (_).
6. Switch the lowercase letter “l” in please with the number “1”.
7. Add an exclamation mark at the end of the passphrase.

0h-dear-sesame,_p1ease_0PEN_up!

Password Managers will help you

It is a software application designed to store and manage online credentials. It also generates passwords. Usually, these passwords are stored in an encrypted database and locked behind a master password.
There are 7 advantages to a password manager:

1. **You don't have to memorize all your passwords anymore.**
2. **They can auto-generate highly secure passwords for you.**
3. **They can alert you to a phishing site and remind you to turn on two-factor authentication (2FA).**
4. **They can help your beneficiaries when you seriously ill or pass away.**
5. **Password managers save time.**
6. **Many password managers sync across different operating systems.**
7. **They help protect your identity.**

Comparison of Password Managers

There are many password managers available on the market. Depending on the choice of program, the passwords are stored either locally on the device or in the provider's infrastructure – often cloud-based – for synchronization across different systems. This excerpt provides a short overview.

1Password	Keeper	LastPass	Bitwarden	KeePassXC
AgileBits Inc. (US)	Keeper Security Inc. (US)	LogMeIn Inc. (US)	Bitwarden Inc. (US)	Community
Released 2006	Released 2009	Released 2008	Released 2016	Released 2016
Cross-platform	Cross-platform	Cross-platform	Cross-platform	Cross-platform
Trialware	SaaS	Freemium	Open Source	Open Source
1password.com	keepersecurity.com	lastpass.com	bitwarden.com	keepassxc.org

You can't go far wrong when deciding to use a password manager. Just try it out. You should consider the following (1) is open source important to you, (2) what platforms do you use and where do you want to use the password manager, and (3) if it is cloud-based, then you should probably check their policies.

Multi-factor (MFA) and Two-factor authentication (2FA)

Multi-factor authentication (MFA) is an umbrella term of two-factor authentication (2FA) in which access authorization is verified by multiple independent characteristics (factors). Those factors are:

1	Knowledge	something only the user knows, e.g., password or pin code
2	Possession	something only the user has, e.g., mobile phone or credit card
3	Inherence	something only the user is, e.g., fingerprint or face id
4	Location	somewhere the user is, e.g., GPS location or specific Wi-Fi

The combination of 2 or more factors makes security a lot stronger.

Wide-ranging 2FA support

By now, 2FA has become a standard that is supported by a large number of companies and websites. This overview shows an excerpt of those that already support it.

BANKING

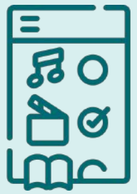
- Bank of America
- Bank of China
- Chase
- Deutsche Bank
- HSBC
- ING
- and many more

COMMUNICATION

- Discord
- Google Chat
- Signal
- Slack
- Telegram
- WhatsApp
- and many more

ENTERTAINMENT

- Discogs
- Google Play
- Plex
- Twitch
- Youtube



GAMING

- Blizzard
- Epic Games
- Rockstar Games
- Steam
- Ubisoft
- Xbox Live
- and many more

HOTELS

- Airbnb
- Booking.com
- Hilton Honors
- Travala
- Vrbo

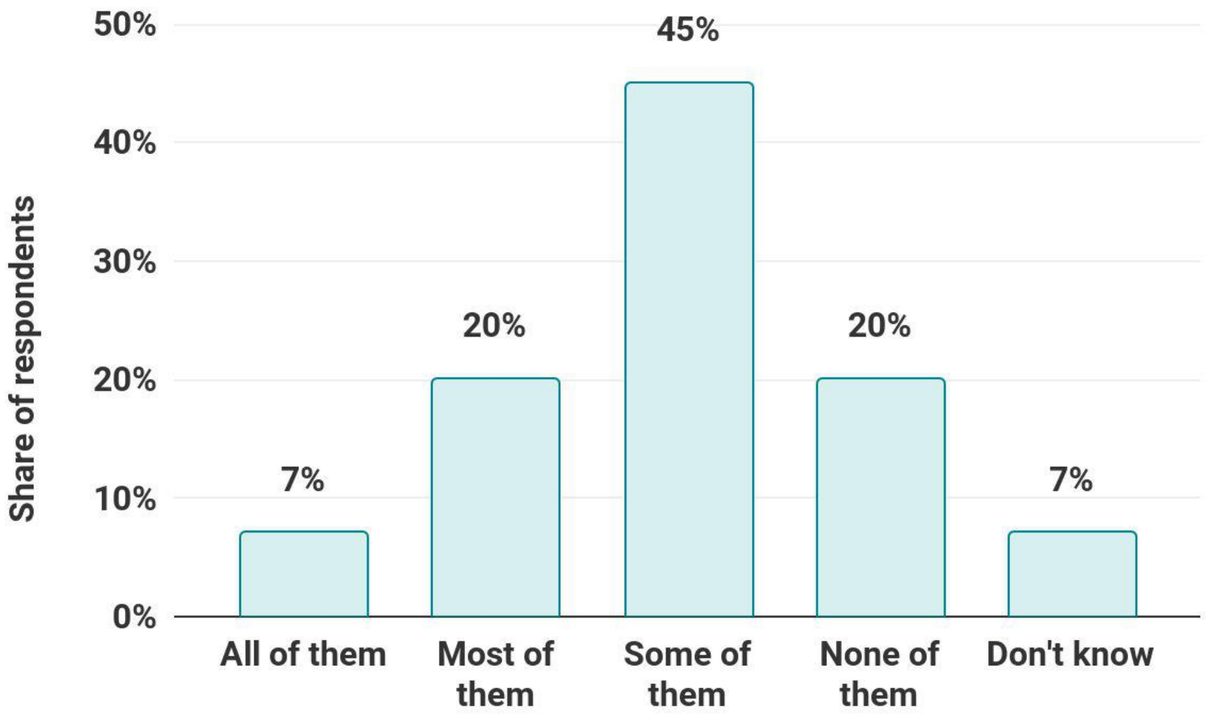
SOCIAL

- Facebook
- Instagram
- LinkedIn
- Reddit
- TikTok
- Twitter
- and many more

Reference: 2FA Directory, (2021)

Use different Passwords for different accounts

A study from 2018 shows that 72% are using the same passwords for multiple accounts, which is an issue if your passwords leak. Only 20% are using unique passwords for their logins.



A password manager can help you to have different passwords for each account.

Reference: YouGov, (2018)

In the light of data breaches

The number of data breaches has increased in recent years. This extract highlights some significant incidents that happened in the last 2 years. It doesn't include password collections, e.g., RockYou2021 with 8.4B records.

CAM4 *03/2020; 11B records*	**LinkedIn** *06/2021; 700M users*	**Sociallarks** *01/2021; 200M records*	**Bonobos** *01/2021; 12M records*	**Easyjet** *05/2020; 9M users*
123RF *11/2020; 8M records*	**Twitch** *10/2021; 7M users*	**Marriott** *03/2020; 5M users*	**Neiman Marcus** *09/2021; 5M users*	**MeetMindful** *01/2021; 2M records*
Pixlr *01/2021; 2M users*	**Graff** *11/2021; 1M records*	**Zoom** *04/2020; 500K users*	**Slickwraps** *02/2020; 370K users*	**Magellan Health** *04/2020; 365K records*

One password per account and 2FA helps you mitigate risk that might arise from such leaks.

Reference: UpGuard, (2021) and CyberNews, (2021)

If you want to check

There are services available that let you check if your data has been leaked. Some password managers use this information to inform you, but you can also manually check it. This extract allows you to review it.

1. Have I been Pwned?
2. CyberNews - Personal Data Leak Checker
3. F-Secure Identity Theft Checker

There are more services available, before using it check what they are doing and read their policies.

5 Takeaways for better security

1. Consider strong passwords for your accounts
2. Use different passphrases for your accounts
3. Let a password manager help you
4. If supported and worth protecting activate 2FA for your accounts
5. Revise your accounts regularly

Thank you!

See more on cybersec.help

References: (1) Icons made by Freepik (2) Cover made by TheDigitalArtist