PASSWORDS AND SOCIAL MEDIA

Digital Security for Journalists and Human Rights Defenders

By Ronalyn V. Olea | Bulatlat, NUJP

HOW SECURE IS YOUR PASSWORD?

https://www.security.org/how-secure-is-my-password/

12 Best Password Cracking Tools in 2022

Rexter Marqueses

Published: January 13, 2022
Updated: August 21, 2022

The technique of retrieving passwords from encrypted data stored in or communicated by a computer system is known as password cracking. The ubiquity of social media sites and online file-sharing has meant it is essential for users to have different passwords for different websites to ensure their safety online. However, keeping track of several different passwords is difficult for some users and often results in passwords being forgotten or misremembered. In this event, password cracking tools can be used to recover lost passwords.

Password cracking tools can also be used by system administrators to check for easily hackable passwords. Although traditionally perceived to be used exclusively for criminal purposes, using password hacking tools to test or recover lost passwords is a legal practice. The best password cracker apps can handle multiple targets simultaneously, are usable on different platforms, and support multiple protocols.

What we cover

1. John the Ripper
2. Hashcat
3. Medusa
4. THC Hydra
5. WFuzz
6. Brutus
7. RainbowCrack
8. L0phtCrack
9. OphCrack
10. Aircrack-ng
11. CrackStation
12. Password Cracker

PASSPHRASES

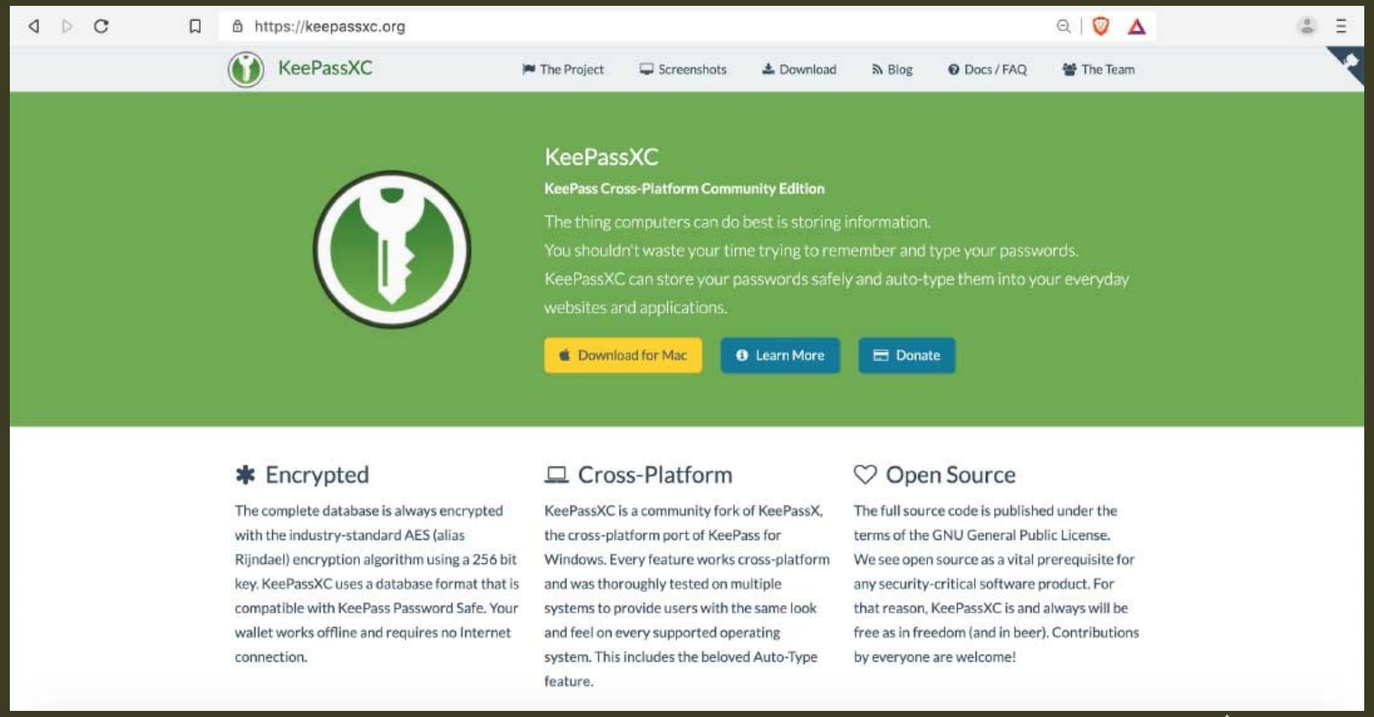
Choose an obscure statement or quotation that will not be easily linked to you by others.
You can use the whole phrase or abbreviate it to create a series of letters and numbers.

For example:“Why is it always so hot outside?” → WiiA50HO?“That toy tiger I had as a kid was the best!” → TtT1hadAak1Dwa5th3B!

Do not use the same password for multiple accounts.

Change your passwords regularly.

PASSWORD MANAGER



Store your passwords in a password manager.
How to use KeePassXC
https://ssd.eff.org/en/module/how-use-keepassxc

Be sure to have a backup stored in an encrypted device.

QUESTIONS WHEN USING SOCIAL MEDIA

- How can I protect my identity, my privacy and my contacts?
- What information do I want to keep private?
- Who do I want to keep it private from?

5 DANGERS OF FACEBOOK

Facebook admits to wrongly sharing user data with third party apps yet again

By Jasmine Gearie July 02, 2020

Facebook tries to save face, again

(Image credit: Shutterstock)

1.Your information is being shared with third parties.

Facebook's mission is to get you to share as much information as it can so it can share it with advertisers.

Every time you take popular quizzes, you authorize an application to be downloaded to your profile that gives information to third parties about you that you have never signed off on.

5 DANGERS OF FACEBOOK

1.Your information is being shared with third parties.

The social media giant estimates the error saw around 5,000 third-party app developers continue to receive information about users who had previously used Facebook to sign into their apps, even if users hadn’t used the app in the past 90 days. (https://www.techradar.com/news/facebook-admits-to-sharing-users-personal-data-with-third-party-apps-yet-again)

5 DANGERS OF FACEBOOK

2. Privacy settings revert to a less safe default mode after each redesign.

Facebook does not [necessarily] notify you of the changes, and your privacy settings are set back to a public default.

5 DANGERS OF FACEBOOK

Facebook: Malware that took over accounts and placed scammy ads a growing risk

The company says it stopped a malware campaign in its tracks, but warned that hackers will keep targeting users of Facebook and other social media platforms.

Laura Hautala Oct. 1, 2020 11:01 a.m. PT

LISTEN · 02:37

3. Facebook ads may contain malware.

Facebook has not been able to screen all of its ads. It hasn't done a great job of vetting which ads are safe and which are not.

5 DANGERS OF FACEBOOK

4. Your real friends unknowingly make you vulnerable

Your security is only as good as your friend's security. If someone in your network of friends has a weak password, and his or her profile is hacked, he or she can now send you malware, for example.
There is a common scam in which someone hacks your profile and sends messages to your friends asking for money - claiming to be you.

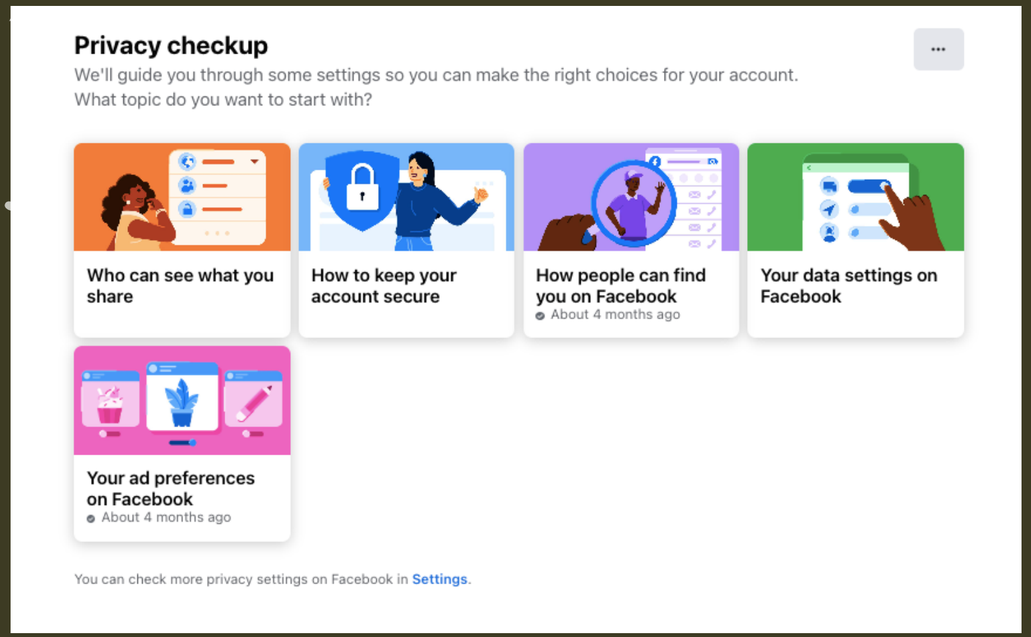
5 DANGERS OF FACEBOOK

5. Scammers are creating fake profiles.

40 percent of all FB profiles are fake.

Source: https://www.cnet.com/news/five-hidden-dangers-of-facebook-q-a/

SECURITY CHECKS



Facebook
https://www.facebook.com/help/443357099140264

Twitter
https://help.twitter.com/en/safety-and-security#ads-an d-data-privacy

Instagram
https://mashtips.com/instagram-privacy-settings/

GENERAL RULES

- Use strong passwords. Change it frequently. Use password manager (Bitwarden or KeePassXC)
- Activate 2FA on all your accounts
- Use separate social media accounts for professional, personal use. Consider using pseudonyms for different activities (buying online, connecting with former classmates, etc.)

GENERAL RULES

- Never log in to 3rd party apps using your social media accounts.
- Set limits and discuss with friends.
- Never access social media from device or network that you don’t trust, or a public computer that may store password or browsing history

GENERAL RULES

- Never log in to 3rd party apps using your social media accounts.
- Set limits and discuss with friends.
- Never access social media from device or network that you don’t trust, or a public computer that may store password or browsing history

VIDEO CONFERENCING

Privacy problems with Zoom:

- Zoom not only tracks your attention, it tracks you.
- Zoom does not use end-to-end encryption
- Zoombombing - by default, allows anyone to share their screen with the participants of a call without permission from the call’s host.

VIDEO CONFERENCING

How you can protect your data:

- Do not use Facebook to sign in: It might save time, but it is a poor security practice and dramatically increases the amount of personal data Zoom has access to.

- Keep your Zoom app updated: Zoom removed the remote web server from the latest versions of its apps. If you recently downloaded Zoom, there’s no need to be concerned about this specific vulnerability.

VIDEO CONFERENCING

How you can protect your data:

- Prevent intruders and Zoombombing on your calls: Before you set up a public Zoom call, go to Settings and turn Screen Sharing to “Host only,” disable “Join Before Host,” disable “Allow Removed Participants to Rejoin,” and disable “File Transfers.” If practical, you should also protect your conference call with a password.

Source: https://protonmail.com/blog/zoom-privacy-issues/

VIDEO CONFERENCING

- Use Jitsi or BigBlueButton

2-FACTOR AUTHENTICATION

The vulnerability of passwords is the main reason for requiring and using 2FA.

90% of passwords can be cracked in less than six hours

Sophisticated cyber attackers have the power to test billions of passwords every second.

2-FACTOR AUTHENTICATION

Two-factor authentication (2FA) is a second layer of security in addition to a password that a user must provide before being granted access to an account or system.

This drastically reduces the chances of fraud, data loss, or identity theft.

AUTHY

Download Authy app on your mobile phone.

Enable 2FA on your Facebook account or Gmail account.

Video tutorial:
https://www.youtube.com/watch?v=7gsBG6Nt21k

Authy for Google and Gmail accounts
https://authy.com/guides/googleandgmail/