

Search 

TechCrunch+
Startups
Venture
Security
Crypto
Apps
Gift Guides
Events
Advertise
More

LastPass says hackers stole cust password vaults

It's time to start changing your passwords

Zack Whittaker [@zackwhittaker](#) / 9:46 PM UTC • December 22, 2022



 **Image Credits:** Bryce Durbin / TechCrunch



password manager giant LastPass has confirmed that cybercriminals stole customers' encrypted password vaults, which store its customer secrets, in a [data breach](#) earlier this year.

In an [updated blog post](#) on its disclosure, LastPass CEO Karim Toubba said the attacker copied a backup of customer vault data by using cloud storage keys stolen from a former employee. The cache of customer password vaults is stored in a “proprietary” format that contains both unencrypted and encrypted vault data, but technical and security details about the proprietary format weren’t specified. The unencrypted data includes [vault-store](#). It’s not clear how recent the stolen backups are.

LastPass said customers’ password vaults are encrypted and can only be unlocked with customers’ master password, which is only known to the customer. But the company says the cybercriminals behind the intrusion “may attempt to use brute force to guess your password and decrypt the copies of vault data they took.”

Toubba said that the cybercriminals also took vast reams of customer data, including email addresses, phone numbers and some billing information.

Password managers are [overwhelmingly a good thing](#) to use for storing your passwords. They should all be long, complex and unique to each site or service. But security experts say it’s a reminder that not all password managers are created equal and can be attacked in different ways. Given that everyone’s threat model is different, no one person’s password requirements are the same as the other.

In a rare situation (not a typo) like this — which we spelled out in [our parsing breach notice](#) — if a bad actor has access to customers’ encrypted password vaults, all they need is a victim’s master password.” An exposed or compromised password vulnerability is the encryption — and the password — used to scramble it.

The best thing you can do as a LastPass customer is to change your current LastPass password to a new and unique password (or passphrase) that is written down in a safe place. This means that your current LastPass vault is secured.

If you think that your LastPass password vault could be compromised — such as if your password is weak or you’ve used it elsewhere — you should begin changing the password for your LastPass vault. Start with the most critical accounts, such as your email account, your cell phone plan account, your bank accounts and your social media accounts, and then move on to the priority list.

The good news is that [any account protected with two-factor authentication](#) will be much more difficult for an attacker to access your accounts without that second factor, such as a texted or emailed code. That’s why it’s important to secure those second-factor accounts like your email accounts and cell phone plan accounts.

[Join](#)

[TechCrunch+](#)

[Login](#)

[Search](#) 

[TechCrunch+](#)

[Startups](#)

[Venture](#)

[Security](#)

[Crypto](#)

[Apps](#)

[Gift Guides](#)

[Events](#)

[Advertise](#)

[More](#)

Parsing LastPass' data breach notice



Two weeks ago, the password manager giant LastPass disclosed its second time this year. Back in August, LastPass found that an employee compromised to gain unauthorized access to the company's development some of LastPass' source code. LastPass CEO Karim Toubba said the reading



TechCrunch

[Join](#)

[TechCrunch+](#)

[Login](#)

Search

[TechCrunch+](#)

[Startups](#)

[Venture](#)

[Security](#)

[Crypto](#)

[Apps](#)

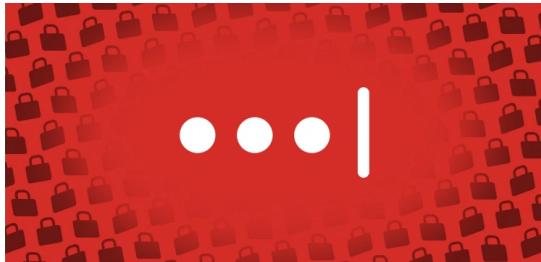
[Gift Guides](#)

[Events](#)

[Advertise](#)

[More](#)

More TechCrunch



[Join](#)
[TechCrunch+](#) [Login](#)

Search 

April 20, 2023 Boston, MA

[Register Now](#)

TechCrunch+

Startups

Venture

Security

Crypto

Apps

Gift Guides

Events

Advertise

More

Sign up for Newsletters

[See all newsletters](#)

- Daily
- Week in Review
- Startups Weekly
- Event Updates
- Advertising Updates
- TechCrunch+ Announcements
- TechCrunch+ Events
- TechCrunch+ Roundup

Email *

<https://tcrn.ch/3Ve0eDr> Copy

Tags

[cybersecurity](#) [data breach](#) [LastPass](#) [password manager](#)

[Join](#)
TechCrunch+ [Login](#)

Search 

TechCrunch+
Startups
Venture
Security
Crypto
Apps
Gift Guides
Events
Advertise
More

Backed by Electrolux, Mila raises at a \$52M valuation to add smarts to fresh air

Haje Jan Kamps

5:32 PM UTC • December 23, 2022

 Market Analysis

While Amazon had a rocky year, AWS remains a reliable cash cow

Ron Miller

5:00 PM UTC • December 23, 2022

Questions linger over Facebook, Twitter, TikTok's commitment to uphold election integrity in Africa, as countries head to polls

Annie Njanja

4:58 PM UTC • December 23, 2022

Clean energy investments may close 2022 hitting new heights, setting stage for lofty 2023

Tim De Chant

3:00 PM UTC • December 23, 2022

Join

TechCrunch+

Login

Search 

Tesla announces a \$300 charging mat that can recharge 3 devices at once

Matt Burns

2:52 PM UTC • December 23, 2022

TechCrunch+

Startups

Venture

Security

Crypto

Apps

Gift Guides

Events

Advertise

More

India's Reliance backs US-based AI startup Exyn in \$35 million funding

Manish Singh

1:30 PM UTC • December 23, 2022

Headcount growth is slowing as startups prepare for worst-case scenarios

Eddie Ackerman

1:00 PM UTC • December 23, 2022

Facebook parent Meta to settle Cambridge Analytica class action lawsuit for \$725M

Paul Sawers

9:55 AM UTC • December 23, 2022

Google appeals India's fine over 'unfair' business practices on Android

Manish Singh

8:06 AM UTC • December 23, 2022

Persistent Jack Sweeney brings back @ElonJet (but delayed) to Twitter

Connie Loizos

6:12 AM UTC • December 23, 2022

Twitter Blue users can now upload 60-minute videos

Ivan Mehta

6:03 AM UTC • December 23, 2022

[Join](#)

[TechCrunch+](#)

[Login](#)

Search

Flipkart and PhonePe complete separation

Manish Singh

5:04 AM UTC • December 23, 2022

TechCrunch+

Startups

Venture

Security

Crypto

Apps

Gift Guides

Events

Advertise

More

Daily Crunch: 2 former SBF associates plead guilty to fraud and are cooperating with US federal prosecutors

Christine Hall, Haje Jan Kamps

11:05 PM UTC • December 22, 2022

The FCC can finally hammer predatory prison phone call companies, thanks to just-passed bill

Devin Coldewey

10:55 PM UTC • December 22, 2022

Tesla's \$7,500 discount feels desperate, and it's giving investors the ick

Rebecca Bellan

8:49 PM UTC • December 22, 2022

'Tis the season for more FTX charges

Jacquelyn Melinek

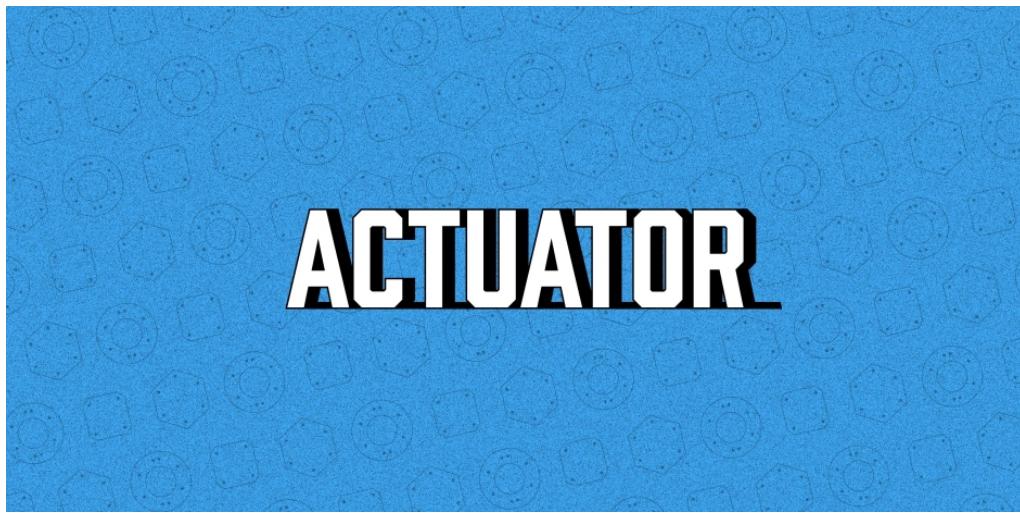
8:00 PM UTC • December 22, 2022

 Investor Surveys

3 Black investors talk about what they're looking for in 2023

Dominic-Madori Davis

8:00 PM UTC • December 22, 2022

[Join](#)[TechCrunch+](#)[Login](#) Search [TechCrunch+](#)[Startups](#)[Venture](#)[Security](#)[Crypto](#)[Apps](#)[Gift Guides](#)[Events](#)[Advertise](#)[More](#)

Notes on robotics research

Brian Heater

7:30 PM UTC • December 22, 2022

 Fundraising

Pitch Deck Teardown: Card Blanch's \$460K deck for its angel round

Haje Jan Kamps

7:00 PM UTC • December 22, 2022

About Legal Trending

TechCrunch

Staff

Contact Us

Advertise

Crunchboard

Jobs

Site Map

Terms of Service

Privacy Policy

TechCrunch+

Terms

Privacy

Dashboard

Code of Conduct

About Our

Ads

Tech

Topics

Tech

Industry

Layoffs

Google

Search On

Event 2022

Amazon

Fall Event

2022

 Facebook

 Twitter

 YouTube

 Instagram

© 2022 Yahoo.

All rights reserved.

Powered by WordPress VIP.

[Join](#)

[TechCrunch+](#)

[Login](#)

Search 

[TechCrunch+](#)

[Startups](#)

[Venture](#)

[Security](#)

[Crypto](#)

[Apps](#)

[Gift Guides](#)

[Events](#)

[Advertise](#)

[More](#)