



## Notice of Recent Security Incident

---

To All LastPass Customers,

I want to inform you of a development that we feel is important for us to share with our LastPass business and consumer community.

Two weeks ago, we detected some unusual activity within portions of the LastPass development environment. After initiating an immediate investigation, we have seen no evidence that this incident involved any access to customer data or encrypted password vaults.

We have determined that an unauthorized party gained access to portions of the LastPass development environment through a single compromised developer account and took portions of source code and some proprietary LastPass technical information. Our products and services are operating normally.

In response to the incident, we have deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm. While our investigation is ongoing, we have achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity.

Based on what we have learned and implemented, we are evaluating further mitigation techniques to strengthen our environment. We have included a brief FAQ below of what we anticipate will be the most pressing initial questions and concerns from you. We will continue to update you with the transparency you deserve.

Thank you for your patience, understanding and support.

Karim Toubba

CEO LastPass

### FAQs

**1. Has my Master password or the Master Password of my users been compromised?**

No. This incident did not compromise your Master Password. We never store or have knowledge of your Master Password. We utilize an industry standard Zero Knowledge architecture that ensures LastPass can never know or gain access to our customers' Master Password. You can read about the technical implementation of Zero Knowledge [here](#).

## **2. Has any data within my vault or my users' vaults been compromised?**

No. This incident occurred in our development environment. Our investigation has shown no evidence of any unauthorized access to encrypted vault data. Our zero knowledge model ensures that only the customer has access to decrypt vault data.

## **3. Has any of my personal information or the personal information of my users been compromised?**

No. Our investigation has shown no evidence of any unauthorized access to customer data in our production environment.

## **4. What should I do to protect myself and my vault data?**

At this time, we don't recommend any action on behalf of our users or administrators. As always, we recommend that you follow our best practices around setup and configuration of LastPass which can be found [here](#).

## **5. How can I get more information?**

We will continue to update our customers with the transparency they deserve.