How many times has LastPass been hacked? Is it still safe to use?

LastPass has suffered multiple data breaches, putting sensitive customer information at risk. So how many times has LastPass been hacked and is it safe to use?

Many of us use password managers to keep our private data safe, with LastPass being one of the most popular options available. But LastPass has suffered multiple data breaches, putting customers' sensitive information at risk.

So how many times has LastPass been hacked and is it safe to use?

1. Violation case in 2015

The first LastPass hack occurred in June 2015, seven years after the company's founding. This high-profile breach exposed LastPass users' emails and master passwords, as well as hint or reminder words used to remember master passwords. The hack came to attention when LastPass detected suspicious network activity, which was soon blocked. However, some damage was done.

In a now-expired note to customers (available on the Internet Archive), LastPass informed users that those using additional layers of security would be safe from the hack. Luckily, the majority of LastPass users use these security methods, meaning only a small portion of customers are affected.

LastPass also stated that it does not believe any user accounts were accessed as a result of the attack but urged users to verify their email addresses or use multiple master passwords for added security.

A few weeks after the hack, LastPass published a blog post stating that the service's security had improved since the hack, with a series of large and small changes made to protect customers, including the introduction of the hardware security module (HSM), which protects LastPass's cryptographic infrastructure.

2. 2021 Tracking Issues

While LastPass was not hacked in 2021, it did encounter problems when its Android app was found to contain third-party trackers. In February 2021, a security analysis app called Exodus Privacy revealed that it found seven trackers in the LastPass Android app, raising suspicions among users. Security researcher Mike Kuketz commented on the findings in a post on the Kuketz IT Security blog, saying that "integrating [ads and trackers] into password manager apps is completely out of the question." cannot happen".

Kuketz also listed seven trackers found in the LastPass Android app, including trackers from Google Analytics, Segment, and AppsFlyer. Granting access to marketing analytics platforms in this way was condemned by Kuketz, who wrote that LastPass's approach was *"extremely questionable from a security perspective"* .

Kuketz emphasized that the LastPass Android app needs to be manually tested to see if the tracker is actively following users. However, the mere presence of trackers was noted by Kuketz as bad practice for an app that prioritizes security.

In response to this criticism, LastPass informed users that it uses analytics tools. LastPass emphasizes that this is done to better understand *"the app's remote crash and error reporting data, as well as high-level usage statistics information to ultimately improve performance, reliability and overall usability of [app]"* .

It is also claimed that the analytics element of the LastPass app is an optional feature that users can turn off in advanced settings. But the tracker's presence in the LastPass Android app nonetheless left a bad impression on security analysts and users.

3. 2022 breach

It took a while for LastPass to experience another cyberattack after the first incident in 2015. In 2022, another attack actually occurred. It's been a particularly rough year for LastPass, with the first hack in August sending shockwaves into 2023.

In early August 2022, LastPass learned of a vulnerability in which hackers compromised a LastPass developer's laptop to steal source code and access the company's cloud-based development platform. Hackers bypassed multi-factor authentication security on the engineer's account by successfully authenticating themselves as users. Although this is a very disturbing incident, the hacker did not obtain customer information.

But a few months later, things got worse. In December 2022, LastPass announced that the August hack gave attackers an opportunity to penetrate more sensitive areas of the service's infrastructure, which was first exploited in November. This time, hackers accessed LastPass customer data, including email and IP addresses, phone numbers, and names. Additionally, several types of user vault data were exposed, including usernames and stored passwords for online accounts.

Needless to say, things won't stop in 2023.

Consequences in 2023

Although 2023 did not see any new hacks of LastPass, there are increasingly worrying reports of breaches taking place in 2022.

In January 2023, LastPass's parent company, GoTo, released a statement about the fallout from the 2022 hack. GoTo's statement explained that several of the company's other services, including Central, Hamachi , Pro, join.me and RemotelyAnywhere, were also targeted by attackers via third-party cloud storage devices. From this device, the attacker stole encrypted backups. Furthermore, GoTo revealed that it found evidence that the encryption keys for some of the stolen backups were also accessed.

In February 2023, LastPass made news headlines again when it was revealed that, between the first hack and the second hack in 2022, attackers committed multiple malicious acts.

As documented in the X post above, hackers in November 2022 compromised the home computer of a senior LastPass developer through a software vulnerability. After hacking the computer, the hackers installed a keylogger, allowing them to see what the developer was typing on the keyboard.

This gives the attacker access to the master password for the developer's LastPass password vault, allowing the attacker access to the vault itself. What's shocking here is that only four senior LastPass developers had access to the company's password vault, and the attackers still successfully targeted one of those four.

Hackers also used user credentials stolen in 2022 to steal $4.4 million in cryptocurrency in October 2023. It is thought the attackers accessed the keys and the cryptocurrency wallet seed phrase in the second breach in 2022, allowing hackers to break into the wallet and withdraw cryptocurrency to their desired address.

LastPass has the full list of data accessed in the 2022 hacks if you want to see all that was exposed as a result of the 2022 incident.

Is LastPass still safe to use?

Even though LastPass has been in operation since 2008, most data breaches and security incidents have occurred in the 2020s. With many security issues that have taken place, it's natural to feel a little nervous when Is using LastPass natural? So is LastPass still safe to use or should you choose another tool?

While using LastPass is more secure than a simple note-taking app or similar storage option, there may be better password managers available today. With so many weaknesses in its security aspect, LastPass has become an overlooked option for many, as they fear not knowing when another breach will occur. With 2022 causing so many problems for LastPass and its users, it's no surprise that some users have turned to password managers that haven't been hacked yet.

Dashlane and NordPass are just two examples of highly reputable password managers that have never suffered a security breach, so it's certainly possible to find a password manager with no customer data or gateways. Employee information was attacked by hackers.

However, LastPass's security problems do not make it an insecure password manager. This app still has many useful features to protect sensitive credentials and is easy to use regardless of whether the user is tech-savvy or not.