PUBLICATION

# The LastPass Lesson: Why Your Company Needs to Care About Password Manager Breaches

**Authors: Alisa L. Chestler**
**March 07, 2023**

**In August 2022, LastPass – one of the largest password managers in the world – suffered a cyber breach resulting in the theft of thousands of password vaults of both individual and corporate users. Password managers are an important security tool, but companies must understand the risks they can pose – and how to mitigate those risks. Even if your company has never used LastPass, your organization may still be at risk.**

One of the most significant risks to cybersecurity is using the same password for multiple accounts. This is because databases containing both hashed and plaintext passwords are frequently compromised, resulting in thousands of usernames and passwords being sold on the dark web almost every day. Malicious cyber actors purchase these databases and run username and password combinations against everything from personal email accounts to corporate networks. As soon as they find a match, such as the same combination for a news subscription as for a corporate email, they're in.

Password management services are used to mitigate this risk. A password manager is a software tool that allows users to securely store and manage their passwords. It generates strong and unique passwords, encrypts and saves them in an encrypted database, and autofills them when users need to log onto websites or applications. Because a single password manager can store the usernames and passwords for every account, a breach of a password management service is especially pernicious.

## LastPass Breach

With a registered userbase of more than 25 million, LastPass is one of the largest password management companies in the world. In August 2022, LastPass initially reported that an "unauthorized party gained access to portions of the LastPass development environment" and "took source code and some proprietary LastPass technical information." In December 2022, LastPass confirmed the threat actor who had compromised its development environment had accessed and copied customer account information and a backup of customer vault data.

In other words, the threat actor stole LastPass's entire trove of usernames and passwords, as well as company names, end-user names, billing email addresses, email addresses, and IP addresses. LastPass users could take some solace in the fact that the database of usernames and passwords was encrypted and can only be opened with the user's master password. In theory, the threat actor would not be able to access their stores of usernames and passwords unless the actor was able to guess their master password – such as by purchasing a cache of previously compromised credentials that were reused and trying each one. However, having stolen and downloaded a local copy of the database, the threat actor could, in theory, continuously run different combinations of usernames and passwords against the database until user vaults unlock.

Were this a typical criminal actor, resource limitations would offer somewhat of a safety net for LastPass users. However, on March 1, 2023, LastPass reported that the initial breach came as a result of a highly skilled and targeted attack against one of its engineers. This attack bore the hallmarks of an advanced persistent threat

(APT), meaning it was very likely a nation-state or other well-resourced operation. With nation-state–level resources, the likelihood that the threat actor can break into the LastPass vaults has increased exponentially.

### Mitigating Corporate Risk

To mitigate risk from this compromise, all users should change any passwords that were stored in LastPass.

However, this, by itself, is not enough.

Before last year's breach, many of the largest professional services companies offered LastPass to their employees as an enhanced cybersecurity measure. In addition, contractors, service providers, and professional services – such as attorneys, accountants, and information technology consultants – are often given usernames and passwords to access company networks and accounts as a necessary requirement for carrying out their services. In turn, many of these usernames and passwords were stored in LastPass and could be used to infiltrate an organization that is not aware the service provider used LastPass.

***Even if your company has never used LastPass, your organization may still be at risk***. Given the broad impact of the LastPass breach, companies of all sizes should conduct an inventory of their active user accounts, including all individual user accounts, administrative accounts, network devices, cloud-based services, and share files. Share files and data rooms are commonly forgotten access points that can leave a company exposed.

- Companies should force a reset of all passwords that have not been changed in the last 90 days *immediately*.
- If users are no longer employed by the company or vendor or professional services are no longer being rendered, suspend those accounts *immediately*.
- If an account has been dormant for at least 90 days, it should be disabled *immediately*.

While password managers are crucial to cybersecurity, they are not a panacea nor are they impenetrable. Because password management services are incredibly lucrative targets for threat actors and APTs, they will continue to suffer breaches. To mitigate this risk, it is important for companies to force password resets in all of accounts at regular intervals. A password should be 16 to 20 characters long and use a mix of upper- and lower-case letters, numbers, and special characters. It is also critical for companies to implement multi-factor authentication that is not tied to an email account or phone number associated with a password management service, like a push notification from a third-party app such as Duo Mobile, Google Authenticator, or Microsoft Authenticator.

For any questions about how the LastPass breach might affect your business or your clients, or how you can prepare for these types of threats, please contact Alisa L. Chestler, CIPP/US, or any member of the Baker Donelson Data Protection, Privacy, and Cybersecurity Team.