Security & Encryption Technology

Safeguarding your data is our top priority. LastPass uses leading technology to ensure the complete security of user data. As a solution built with local-only encryption, your master password is never shared with LastPass, so only you ever have access to the sensitive information you store in your LastPass account.

Private Master Password

Users create an account with an email address and a strong master password to locally-generate their unique encryption key. The master password, and the keys used to encrypt and decrypt user data, are never sent to LastPass' servers, and are never accessible by LastPass. The encrypted data is meaningless to us and everyone else without the decryption key, and the components that make up your key remain local.

Local-Only Encryption with Leading Algorithms

We've implemented AES-256 bit encryption with PBKDF2 SHA-256 and salted hashes to ensure complete security in the cloud. User data is encrypted and decrypted exclusively at the device level. Data stored in the vault is kept secret, even from LastPass. This means that your sensitive data does not travel over the Internet nor does it ever touch our servers, only the encrypted data does. We've taken every step possible to ensure that your data is safely stored and synced in your LastPass account. This is the same encryption algorithm that is used by the US Government to protect its top-secret data.

Two-Factor Authentication

Two-factor (multifactor) authentication adds extra security to LastPass accounts by requiring a second login step before authorizing the user. LastPass integrates with over a dozen services provided by the best two-factor authentication vendors available.

An Architecture Designed for Security

Our policy of never receiving private data that has not already been locked down with a LastPass Master Password (which we never receive and will never ask for) radically reduces attack vectors. We use firewalls and best practices to protect the servers and service, as well as regular third party audits. However, our best line of defense is simply not having access to data even if someone were able to hack their way in. If LastPass can't access it, hackers can't either.

Transport Layer Encryption

LastPass uses SSL for secure data transfer between a device and the servers, adding another layer of protection to the encrypted data blob - even though the vast majority of data being sent is already encrypted with AES-256 and is unusable to both LastPass and any party listening in to the network traffic.

Password Strengthening with PBKDF2 SHA-256

LastPass has multiple layers of protection in place that will lock down the device in cases of a brute-force attack, based on a deep and diverse set of criteria. PBKDF2 is a leading hashing algorithm to strengthen the master password and encryption key against large-scale, brute-force attacks. This makes it difficult for a computer to check that any one password is the correct Master Password during an attack. The standard implementation of PBKDF2 uses SHA-1, a secure hashing algorithm. SHA-1 is faster, but its speed is a weakness in that brute-force attacks can likewise be performed faster. LastPass has opted to use SHA-256, a slower hashing faster. LastPass has opted to use SHA-256, a slower hashing algorithm that provides more protection against brute-force attacks. By default, LastPass performs 5,000 rounds of the function to create the encryption key, before a single additional round of PBKDF2 is done to create your login hash. We've taken every step to ensure our users' security and privacy.

SOC-2 Attestation

The SOC-2 is a detailed review of the controls and processes in place to ensure our products and systems are secure and reliable, ensuring proper confidentiality and availability of our systems.

Enterprise Security Options

LastPass also offers an array of advanced security options that let you add more layers of protection for your organization. Over 50 configurable security policies allow LastPass Enterprise Admins to create a custom security environment.

All rights reserved, LastPass © 2017