Is my data in LastPass secure?

Q: Is my data in LastPass secure?

Answer

At LastPass, your security and privacy are our their top priority - that's why they have taken every step possible to ensure that your data is safely stored and synced in your LastPass account. This has been accomplished by using 256-bit AES implemented in C++ and JavaScript (for the website) and exclusively encrypting and decrypting on the local PC. This means that your sensitive data does not travel over the Internet nor does it ever touch our servers, only the encrypted data does. This is the same encryption algorithm that is used by the US Government to protect its top-secret data.

Your encrypted data is actually meaningless to LastPass and to everyone else without the decryption key. This key is created from your email address and Master Password. Your Master Password is never sent to LastPass or MIT, only a one-way hash of your password when authenticating, which means that the components that make up your key remain local. LastPass also offers an array of advanced security options that let you add more layers of protection for your organization.

Highlights

- All sensitive data is encrypted locally
- They use government-level encryption
- Only your users know the key to decrypt their data
- No more using your browser’s insecure password manager

See Also

- LastPass Landing Page