LastPass Security: What You Need to Know

Security is our mission at LastPass. At every step, we've designed LastPass to protect what you store, so you can trust it with your sensitive data. We keep your information safe with:

- **A proven security model**, setting the standard for transparency and best practices
- **Local encryption**, so sensitive information is obscured before it's synced to LastPass
- **Powerful security features**, to give you tools to protect against threats and attacks

Here's an introduction to how LastPass encrypts data, hardens our service, and improves your security.

Proven Security Model

We utilize best practices to protect our infrastructure, including regularly upgrading our systems, as well as utilizing redundant data centers to reduce the risk of downtime or a single-point-of-failure. LastPass is market-tested by over 32,000 companies, including Fortune 500 and leading tech enterprises. Our customers trust us in part for our proven security model, including:

- **Service Organization Control 2 (SOC 2) Type II compliance**: Service Organization Control 2 (SOC 2) Type II compliance: Few password managers have achieved the SOC 2 Type II, a detailed review and validation of our controls and processes to confirm our products and systems are designed to be secure and reliable. As a widely-recognized "gold standard" for software companies, completing and maintaining the SOC 2 is one of the many ways we demonstrate our commitment to security and service availability.
- **Regular audits and penetration tests**: We engage trusted, world-class, third-party security firms to conduct routine audits and testing of the LastPass service and infrastructure. Vulnerability scans are run daily against all LastPass servers, and a detailed internal penetration test is performed quarterly.
- **TLS for secure data transfer**: Even though sensitive data is already encrypted with AES-256, the TLS protocol secures the connection to LastPass to further protect a user's data from any party listening in to the network traffic (man-in-the-middle attacks).
- **Bug bounty program**: LastPass has established a positive relationship with the security research community. Our product and customers benefit from the attention we receive from top security researchers, and we value the work they contribute. Our bug bounty program incentivizes responsible disclosure and improvements to our service: https://bugcrowd.com/lastpass
- **Reliable service**: LastPass is operated out of multiple, geographically-distributed facilities, any one of which can handle all customer traffic for redundancy.
- **Transparent incident response**: Security is our highest priority at LastPass – our team reacts swiftly to investigate, verify, and resolve reports of bugs or vulnerabilities according to our incident response plan. We continue to earn our community's trust by looking to our community to challenge our technology, reacting promptly, and communicating transparently.

Secure Product Architecture

Securing an account begins the moment it's created. When a LastPass user creates their master password, it's used to generate a unique encryption key. The master password and the encryption key stay local – they are never sent to or shared with LastPass. The encrypted data is meaningless without that key. LastPass has been designed to keep your sensitive data safe by utilizing the following best practices:

- **End-point encryption**: LastPass is devised to allow only the user to decrypt and access their vault. Encryption happens exclusively at the device level, rather than on LastPass' servers. Sensitive data is encrypted before being synced to LastPass for safe storage.
- **256-bit AES encryption**: This algorithm is widely accepted as impenetrable – it's the same encryption type utilized by banks and the military.
- **PBKDF2-SHA256 for brute-force attacks**: PBKDF2 strengthens the master password and encryption key against large-scale, brute-force attacks by increasing the amount of time it takes to make even one guess for a password. LastPass uses SHA-256 and performs 100,000 rounds of PBKDF2 to create the encryption key, before creating the user's login hash. By slowing down brute force attacks, PBDKF2 makes it difficult to try cracking even just one master password.

- **Private master password**: Our best line of defense is simply not having access to sensitive vault data. That's why LastPass does not send or store the master password. We believe that if LastPass can't access your data neither can hackers.

Powerful Security Features

We not only go to extraordinary lengths to keep vault data safe, we also empower our customers to take security into their own hands, by offering features and functionality to augment the security of their account and improve overall security posture, including:

- **Multifactor authentication**: Add extra security by requiring a second login step before authorizing a user. LastPass Authenticator provides push-based verification for a safe, streamlined user experience. We also integrate with leading authentication providers.
- **Business controls**: Over 100 configurable policies help create a custom security environment, at a global or granular level, including restricting access to trusted locations. The admin dashboard gives visibility into the password security of the entire organization.
- **Automatic locks**: LastPass can automatically log out to make sure your data is safe from prying eyes when you walk away from your computer or even if a device is lost.
- **Password audits**: Scan the passwords in your vault to identify and replace any weak, reused, compromised, and old passwords.
- **Phishing protection**: LastPass will only fill in passwords on the sites you've saved and have trusted.

For more in-depth technical details and additional information about our security model, please see the LastPass Technical Whitepaper.