LastPass Security and Compliance

At LastPass, your security and privacy are our top priority - that's why we've taken every step possible to ensure that your data is safely stored and synced in your LastPass account. We've accomplished this 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 meaningless to us 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, 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.

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. To increase the security of your master password, LastPass utilizes a stronger-than-typical version of Password-Based Key Derivation Function (PBKDF2). At its most basic, PBKDF2 is a "password-strengthening algorithm" that makes it difficult for a computer to check that any one password is the correct master password during a brute-force 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 algorithm that provides more protection against brute-force attacks. LastPass utilizes the PBKDF2 function implemented with SHA-256 to turn your master password into your encryption key. By default, LastPass performs 500 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 user’s security and privacy.

On Windows, the LastPass installer helps find insecure passwords stored on a user’s computer so that they can be saved securely in LastPass, eliminating their easy access by malicious software. As an additional precaution LastPass uses SSL exclusively for data transfer - even though the vast majority of data being sent is already encrypted with 256-bit AES and is unusable to both LastPass and any party listening in to the network traffic. 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, but 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.

Strengthen Compliance Through Controlled Access and Monitoring

Safeguarding your customer’s personal information is a considerable challenge in today’s environment of remote offices, virtual employees, the increased use of Web services, and the increased incidence of cyber-attacks. Each regulatory framework is different, but HIPAA, PCI, SOX and GLBA all call for highly defined processes relative to employee access to data, the ability to track this access, and retention of these records. LastPass helps support corporate compliance efforts by:

- Empowering administrators to control employee access to specific tools and sites

    - Employers can impose specific criteria around the strength and length of the master passwords of their employees.
    - Employers can mandate the use of multi-factor authentication for login to LastPass.
    - Employers can lock down access to LastPass based on IP Address and/or device. Access can be restricted for all employees, or an elected sub-set.
    - With LastPass Shared Folders, Administrators can allocate logins to users as either hidden or visible. Hidden passwords can only be utilized through LastPass auto-fill. Every login event is then captured and retailed in the Login Reports.
- Monitoring and logging all access by both employees and administrators
    - The LastPass Login Report captures (1) username, time date stamp, IPaddress and site name for every login, (2) formfill events, (3) and all username and password updates, that are conducted using LastPass.
    - The Shared Folders Report captures a detailed record of every Shared Folder created within the company, including: (1) assigned users, (2) access rights and permissions of each user relative to each folder, (3) full list of sites and tools shared with the folder.
    - The Admin Events Report tracks administrator activity conducted with the Enterprise Console such as (1) new account created, (2) user account terminated, (3) policy edit or assignment. This report includes the name of the administrator, time/date stamp, IP Address and event type.
- Retaining access records for a minimum of three years
    - Each report is retained on our servers for a period of no less than 3 years.
    - Reports can be filtered by user, data range, and can be exported to Excel.

Safely Sharing Accounts With Others

LastPass uses public/private key cryptography - specifically RSA from Crypto++ and jsbn - to allow users to share their accounts with trusted parties, without ever sharing it with LastPass. The distinguishing technique used in public-key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys - a public encryption key and a private decryption key. Messages are encrypted with the recipient's public key, and can be decrypted only with the corresponding private key. This process is, of course, completely automated with no action required by the end user.

Account Recovery

With 'account recovery', we store an encrypted version of the user's encryption key on their hard drive and store an encrypted version of the key to decrypt the encryption key on our server. The encrypted value on their hard drive is useless without the encrypted key on the server. The encrypted key on our server is useless to us as we do not have the key to decrypt it. We force the end user to prove they are who they claim to be by validating their email and thereafter deliver the encrypted key to the user -- they then decrypt the key and use it to decrypt their encrypted key to gain access to a forced password reset module.

Availability

LastPass was built on the belief that users must always have access to their data – anywhere, anytime. We've accomplished this in multiple ways: first, we have 2 distinct data-centers in production service at

all times. Both are tier 1, SAS-70 certified. Second, we store the user's encrypted data on the local PC at login, so that if LastPass.com cannot be reached, the user will still have full access to the add-on and to their stored accounts. The website can be used without installation of the add-on (the encryption and decryption happens in JavaScript), but we take advantage of faster encryption in the add-ons when available. LastPass also offers user access through the mobile site m.lastpass.com.

Off Site Backups

LastPass keeps daily local backups as well as a daily off site backup hosted through Amazon's S3 service. Although private data is already encrypted on our servers, as an additional precaution backups are also encrypted with GPG.

Automated Testing

LastPass uses Paros to help verify it hasn't made common mistakes that could result in a XSS or SQL Injection attack, and Funkload to verify performance and create functional tests that are run by Nagios. Microsoft's Application Verifier and other tools are used to help identify common problems in the IE add-on as well as a number of Mozilla tools that are used to test the Firefox add-on.