Security Practices

Security and Privacy

Password Boss was designed with the highest level of security in mind to ensure that users are the only ones with access to their data. One the following pages you will find a technical overview of the security steps and process Password Boss has implemented to protect the data that users store in Password Boss, as well as security for the minimal personal account data that Password Boss stores to identify users.

Overview

MASTER PASSWORD: The only way to access *any* data in Password Boss is with the Master Password. Each user creates a unique Master Password that is not stored or transmitted anywhere. Without knowing the Master Password, all of the data within Password Boss remains securely encrypted and inaccessible by anyone.

BANK-GRADE ENCRYPTION: All your passwords and personal information stored in Password Boss are encrypted with 256-bit AES encryption (with 64,000 rounds of PBKDF2 salt), the same level of security used by banks and governments to protect sensitive data. This type of encryption has never been cracked.

LOCAL-ONLY DECRYPTION: All usernames, passwords and personal data that are stored in Password Boss are encrypted and decrypted locally. At no time is any sensitive data ever sent to Password Boss servers without being fully secured and encrypted. Password Boss never has any access to your sensitive data.

TWO-STEP VERIFICATION: Password Boss adds an extra layer of security to user data by adding a two-step verification process that requires both the Master Password and a rotating code from a mobile phone to access any account data. This greatly increases the security of a Password Boss account.

SECURE CLOUD BACKUPS: Password Boss automatically backs up an encrypted copy of users data to a secure cloud storage location, keeping passwords and personal information protected even when a device is lost or stolen. The information within the backed-up data is completely inaccessible to anyone without the unique Master Password that the user created.

THEFT PROTECTION: A remote-delete feature lets users quickly remove Password Boss data from a lost or stolen device, while still preserving an online backup copy of the data.

SECURE SHARING: Passwords and other data that users share are encrypted with unique 2048-bit RSA public/private keys. Only the sender and the recipient have access to the shared data.

SECURITY ALERTS: Password Boss sends users up-to-date security notifications and actionable advice when security breaches occur. For example, consumers will receive a notification to change a password when a site they have an account with has had a security breach.

GLOBAL STORAGE: Users control their security by choosing where in the world they want to store their encrypted data, a feature that is unique to Password Boss. Users can choose from locations in the U.S., Europe, Asia, South America or Australia, and move their data anytime they like.

TOUCH ID AND FINGERPRINT SUPPORT: Password Boss mobile apps let users quickly unlock their Password Boss account with a fingerprint instead of entering the Master Password or PIN code.

Client-Side Data Encryption and Decryption

All Password Boss user data is encrypted and decrypted locally. Access to the user's data requires a Master Password that the user chooses at the time the account is created. The Master Password is never stored or transmitted anywhere. Password Boss employees do not have access to a user's Master Password, and if a user forgets their Master Password, Password Boss employees do not have the ability to reset the Master Password.

- The Master Password is used to generate a unique encryption key using PBKDF2 (OpenSSL's PKCS5_PBKDF2_HMAC_SHA1). The Password Boss client database is initialized with a unique random salt in the first 16 bytes of the file. This salt is used for key derivation and it ensures that even if two databases are created using the same password, they will not have the same encryption key. This process uses 64,000 iterations for key derivation.

- The key used to calculate page HMACs is different than the encryption key. It is derived from the encryption key and using PBKDF2 with 2 iterations and a variation of the random database salt.

- The algorithm is 256-bit AES in CBC mode. Each database page is encrypted and decrypted individually. The page size is 1024 bytes.

- Each page has its own random initialization vector. The IV is generated by OpenSSL's RAND_bytes, and is stored at the end of the page. IVs are regenerated on write so that the same IV is not reused on subsequent writes of the same page data.

- Every page write includes a Message Authentication Code (HMAC_SHA1) of the ciphertext and the initialization vector at the end of the page. The MAC is checked when the page is read back from disk. If the ciphertext or IV have been tampered with or corrupted the HMAC check will report the issue.

- The database is encrypted using the peer-reviewed OpenSSL libcrypto for all cryptographic functions.

Network Security

The Password Boss servers are hosted at AWS for maximum security. All servers are monitored 24/7 using both Amazon monitoring, 3rd party services, as well as custom monitoring developed by Password Boss. The data center has the following Certifications:

- PCI DSS Level1
- SOC 1 / SOC 2 / SOC 3
- ISO 270001

Security Architecture

- The encrypted copies of user account databases, the client databases, are only accessible via AWS keys or a temporary download link that is authenticated and verified via our internal API. Access to the API is also fully secured with username and password protection.

- We maintain a minimal set of personal information to identify users of the Password Boss application. The databases used to store this information are encrypted, protected with a strong-password policy, and access is IP restricted.

- All communications with our servers, and between our servers, is done over HTTPS. Access to all servers is IP restricted to prevent man in the middle attacks.

- Application and database servers are isolated in separate security zones that allows us to only expose necessary services to the Internet.
- All servers are hardened according to NIST best practices.
- Role-based security is in place to limit the access a person or system has to non-essential parts of the Password Boss infrastructure.
- All access to our infrastructure requires 2-step verification to further protect against unauthorized access to the Password Boss systems.

Sharing Data

Password Boss makes it easy for users to share data with people you trust. You have complete control over who receives the information as well as how long they have access to it.

All shared data is secured using a unique key with a randomized IV, encrypting it with 256 bit AES in CBC mode and computing SHA256 HMAC on the ciphertext. The data is then encrypted using 2048 bit RSA keypairs prior to being transferred between users.