How your sign-in credentials are stored and protected by OnceHub

Last Modified on Apr 30, 2020

Protecting the confidentiality, integrity, and availability of data processed through our services is a fundamental objective of the OnceHub security program. We employ strong technical safeguards to ensure that data is protected and the risk of exposure is minimized.

Encryption

All data, including sign-in credentials and passwords, are encrypted in transit and at rest using the Transparent Data Encryption service (TDE) provided by Microsoft Azure. TDE uses strong cyphers (AES-256) and the keys are managed by Microsoft Azure Management.

To learn about all our security processes, visit the OnceHub Trust Center.

Cryptographic Hashing

Your OnceHub password is stored in our cloud database using Secure Hash Algorithm 2 (SHA-2), a set of cryptographic hash functions designed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

Learn more about SHA-2

Third-party integration credentials

When you enter your credentials to connect third-party apps to OnceHub, your password is encrypted with AES-256 (Advanced Encryption Standard) and stored in our cloud database.

Learn more about AES-256 encryption