PassHub

Security Business

MORE THAN YOUR AVERAGE PASSWORD MANAGER

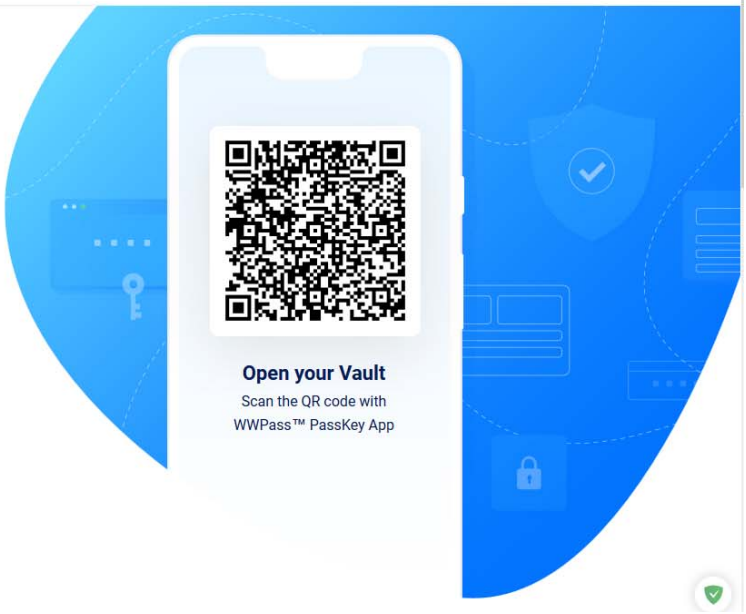
Organize all your credentials and sensitive files for instant and secure access anytime you need them. Always free for everyone *

Watch video

WWPASS PASSKEY APP IS YOUR KEY TO ACCESS PASSHUB

Scan the QR code with **WWPass PassKey app** to open your PassHub vault

Get started



WHAT YOU CAN DO WITH PASSHUB

Store

your credentials,
notes & files securely

Access

your credentials & files
anywhere & anytime

Organize

your credentials & files
the way you want

PassHub Security

STRONG MULTIFACTOR AUTHENTICATION. NO USERNAMES OR PASSWORDS

Passhub implements WWPass™ authentication technology. The cryptographic authenticator, which is called a Passkey, comes in multiple forms including smartcards, USB tokens or mobile apps and is 'something you have' which is used as the first factor when logging in. For a second factor, a PIN is sometimes used. This PIN is optional and whether or not it is required is up to the company running the site you are logging into. This PIN is 'something you know.' The Passkey authenticator is 'one key for many doors' (one-to-many), which does not require a password or even username.

CLIENT-SIDE AND END-TO-END ENCRYPTION

Along with WWPass™ strong authentication, PassHub.net also features client-side encryption. Client-side encryption means that all sensitive data is ciphered with a Passkey in the user browser. No meaningful information is accessible on the server side. We use asymmetric cryptography to send crypto keys to your peers, thus providing end-to-end encryption. When a user signs in, the browser gets an encryption key, specific for each user-web site pair.

HIGH ENTROPY

Unlike other password managers, Passhub does not use key derivation based on passwords (PBKDF). In a passkey, authentication credentials are totally independent of data encryption mechanism, thus providing 256-bit entropy for symmetric keys. High entropy means it is practically impossible to guess or brute-force the secret keys.

STANDARD AND OPEN SOURCE CRYPTOGRAPHY

Passhub employs Web Crypto JavaScript API, which is specified by W3C. Web Crypto API establishes new standards for security and speed for in-browser cryptography. While all modern browsers support this spec, Passhub relies on open source Forge crypto library as a fallback on older devices.

STANDARD ENCRYPTION ALGORITHMS

PassHub only uses NIST approved algorithms, which include: AES-GCM 256 bits and RSA-OAEP.

WEB SERVICE OR ON-PREM DEPLOYMENT

Passhub employs Web Crypto JavaScript API, which is specified by W3C. Web Crypto API establishes new Passhub.net is a free web service available to every individual. The service does not collect any private information. Each user only needs an anonymous Passkey to create a Passhub account.
For companies where security policy prohibits external services, a custom dedicated version of PassHub is available for installation on company premises or in the company's cloud. With the custom dedicated version of PassHub, user access and activity are controlled by a company site administrator. As a protection against Insider breaches and abuse of admin privileges, the site admin cannot read user sensitive data.

HIGH AVAILABILITY

PassHub features a distributed server architecture with database replication and multi-head Web servers to provide reliable 24 x 7 availability.

For more technical details, please download PassHub Security Explained white paper.