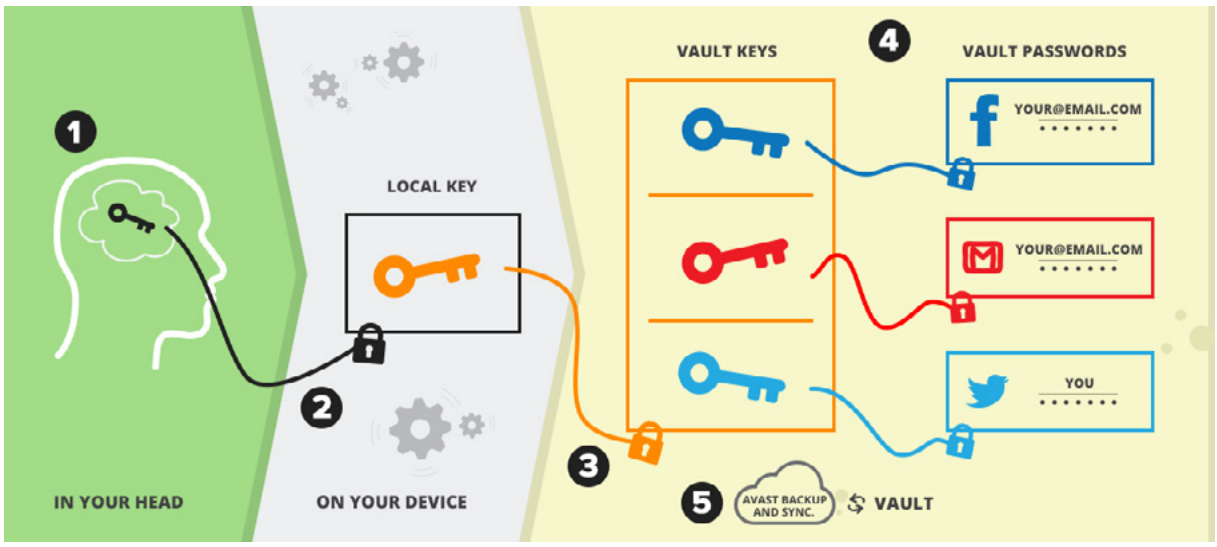
Avast Passwords Security Model

Avast Passwords is focused on ensuring both security and privacy, letting you backup and synchronize your passwords without fear. This document will shed light on our privacy and security model.

The below diagram shows how the master password only you know unlocks the actual passwords that log you in to your different accounts.



1. Your Master Password – which only you know and which is not stored anywhere on your device or on Avast's servers – unlocks Avast Passwords on your device and protects everything stored inside the app. (You can use the same Master Password across all your devices or create a different one for each device as you see fit.)

2. When you unlock Avast Passwords on your device, a series of highly secure steps using random numbers (salt) and secret keys (key derivation and decryption) unlocks an encrypted, randomly generated, device-specific encryption key that's stored locally on the device and nowhere else.

3. This local key unlocks the password vault on your device by performing yet another series of highly secure steps as above.

4. The vault protects the individual encryption keys that unlock each of your account login credentials (i.e., username/password pairs), which are also stored in the vault in encrypted form. Each account requires a different, randomly generated and encrypted key.

5. If you have Backup & Synchronization activated, your encrypted usernames/passwords pairs are also stored on Avast's servers, but since your local key is not stored on Avast's servers, Avast has no way of accessing these usernames/passwords pairs.

How strong is the encryption?

Short answer: Very!

Avast Passwords uses a combination of symmetric and asymmetric cryptography. Encryption with AES-256 provides military-strength confidentiality for your login credentials. ECDH (Elliptic curve Diffie-Hellman) key agreement and AES-256 allow for secure synchronization of encrypted passwords between devices, while permitting a different Master Password for each device. Each key uses 256-bit security, which means that all the energy of the entire universe wouldn't be enough to break it open. Since the local vault key never leaves your device and is stronger than any Master Password a human can come up with, your passwords are fully protected both on your device and when synchronized.