



Whist

MYSTERIOUSLY SEALED

A private vault for passwords, cards, and files – local to your Mac, iPhone, and iPad. No account, no cloud, no one reading along.

Mac · iPhone · iPad · Version 1.2

WHY WHIST IS DIFFERENT

No frills

Most password apps these days want to be more than you actually need. They autofill everything, keep suggesting new passwords, nag you every few weeks that entry number 87 could really use another change, and quietly send everything to a cloud you'll never actually see.

Whist deliberately doesn't do any of that.

At its core, Whist does almost the same thing as all the others: it collects passwords and card details. The difference is in what it doesn't do. Whist runs entirely locally on your own device. It doesn't need a server, because there isn't one. It doesn't sync anything automatically, doesn't copy anything to the clipboard on its own, doesn't suggest a new password you never asked for, and doesn't keep pestering you to change something that's already working fine.

Everything that happens, you set in motion yourself. An entry only ends up somewhere once you save it. A password is only copied once you tap "Copy". Nothing runs in the background without you wanting it to.

That's not a missing feature. That's the whole idea: a simple, fast, secure place to keep things – no frills, no automation, no one else having a say but you.

IN SHORT

What Whist does

Whist brings together three things that are normally scattered across several apps and slips of paper: credentials, card details, and a handful of important files. Everything stays on your own devices – Whist has nothing to send to a server, because there isn't one.

Passwords Credentials sorted by category, with a strength meter, generator, and favorites.	Cards Scan credit/loyalty cards with the camera or enter them by hand, PIN field included.
File Vault A second, independently encrypted area for documents and images.	Security Face ID/Touch ID, automatic lock, encrypted backup – all configurable.

AREA I

Passwords

Every entry belongs to a category – Website, Device, Access Code, or Other. For “Device”, Whist automatically shows the right fields for IP address and network name instead of a username. The list groups every entry by category and can be filtered by search or narrowed down to favorites.

- Password strength is shown live while typing (weak to very strong)
 - One-tap generator for random, secure passwords
 - Copy/paste buttons right next to the username and password fields
-

AREA II

Cards

The camera recognizes card number, expiry date, and name automatically – even on embossed cards whose digits are split across several lines. Recognition runs entirely on the device; nothing is transmitted. Before saving, the photo can still be rotated and the recognized values checked.

- Warns if a card with a number that's already stored is scanned again
 - Its own PIN field, stored independently from the card number
 - Card number is displayed in blocks of four, just like on the real card
-

AREA III

File Vault

The File Vault is deliberately kept separate from the rest of the app: its own password, its own AES-256 encryption, independent of Face ID. Anyone who opens the app via Face ID still can't reach the stored files without this second password. Meant for brokerage documents, ID photos, crypto seed phrases, or anything else that deserves an extra hurdle.

- Add images from the photo library or any file from the file browser
 - Direct Quick Look preview, without exporting the file first
 - Five wrong attempts lock the area for 5 minutes and trigger a notification
-

AREA IV

Security & Backup

Access & Lock

Face ID/Touch ID opens the app; anyone who'd rather turn that off sets a fallback password instead. A configurable auto-lock (1, 5, or 10 minutes) reliably closes Whist once it's in the background – even if the device itself was never locked.

Backup

A backup can be exported at any time as an independently encrypted file – with a password you choose yourself, separate from the app's own access. That lets the whole collection travel safely between Mac and iPhone via AirDrop or Mail, with no automatic cloud sync involved.

What “local” means for Whist

Passwords and cards live in Apple's own device Keychain – the same protected storage iOS and macOS themselves rely on.

The File Vault and backup export are additionally encrypted with their own AES-256 key derived from your password.

There is no Whist server. Nothing leaves your device unless you export it yourself.

APPEARANCE

Customizable, not unlimited

Appearance (System/Light/Dark), a fixed set of accent colors, text size, and bold text can all be adjusted centrally in Settings – along with a background chosen from ready-made gradients or your own photo. The interface itself is fully bilingual (German/English) and switches without restarting.

SYSTEM REQUIREMENTS

Devices & Platforms

Device	Face ID / Touch ID	Note
Mac	Touch ID, where available	standalone app, no browser needed
iPhone	Face ID / Touch ID	card scanning needs camera access
iPad	Face ID / Touch ID	same features as on iPhone

Whist – Version 1.2

© 2026 Heiko Imiolczyk