



Whist

MYSTERIOUSLY SEALED

Ein privater Tresor für Passwörter, Karten und Dateien – lokal auf deinem Mac, iPhone und iPad. Kein Konto, keine Cloud, kein Mitlesen.

Mac · iPhone · iPad · Version 1.2

WARUM WHIST ANDERS IST

Kein Schnickschnack

Die meisten Passwort-Apps wollen heute mehr sein, als du eigentlich brauchst. Sie füllen automatisch aus, schlagen ständig neue Passwörter vor, erinnern dich alle paar Wochen daran, dass Eintrag Nummer 87 doch mal wieder geändert werden sollte, und schicken im Hintergrund alles in eine Cloud, die du nie zu Gesicht bekommst.

Whist macht das bewusst nicht.

Im Kern tut Whist fast dasselbe wie all die anderen: Es sammelt Passwörter und Kartendaten. Der Unterschied liegt darin, was es nicht tut. Whist läuft komplett lokal auf deinem eigenen Gerät. Es braucht dafür keinen Server, weil es keinen gibt. Es synchronisiert nichts automatisch, kopiert nichts von sich aus in die Zwischenablage, schlägt dir kein neues Passwort vor, das du nicht angefordert hast, und mahnt dich nicht ständig, etwas zu ändern, das gerade gut funktioniert.

Alles, was passiert, hast du selbst angestoßen. Ein Eintrag landet erst dann irgendwo, wenn du ihn speicherst. Ein Passwort wird erst dann kopiert, wenn du auf „Kopieren“ tippst. Nichts läuft im Hintergrund, ohne dass du es willst.

Das ist kein fehlendes Feature. Das ist die Idee dahinter: ein einfacher, schneller, sicherer Ort zum Sammeln – ohne Schnickschnack, ohne Automatik, ohne dass irgendjemand außer dir mitredet.

KURZ GESAGT

Was Whist macht

Whist sammelt drei Dinge, die man normalerweise über mehrere Apps und Zettel verstreut: Zugangsdaten, Kartendaten und einzelne wichtige Dateien. Alles bleibt ausschließlich auf deinen eigenen Geräten – Whist schickt nichts an einen Server, weil es keinen gibt.

Passwörter Zugangsdaten nach Kategorie sortiert, mit Stärke-Anzeige, Generator und Favoriten.	Karten Kredit-/Kundenkarten per Kamera einscannen oder von Hand eintragen, inkl. PIN-Feld.
Datei-Tresor Ein zweiter, eigenständig verschlüsselter Bereich für Dokumente und Bilder.	Sicherheit Face ID/Touch ID, automatische Sperre, verschlüsseltes Backup – alles einstellbar.

BEREICH I

Passwörter

Jeder Eintrag gehört zu einer Kategorie – Webseite, Gerät, Zugangscode oder Sonstiges. Bei „Gerät“ zeigt Whist automatisch die passenden Felder für IP-Adresse und Netzwerkname statt Benutzername an. Die Liste gruppiert alle Einträge nach Kategorie und lässt sich per Suchfeld durchsuchen oder auf Favoriten eingrenzen.

- Passwort-Stärke wird beim Eintippen direkt angezeigt (schwach bis sehr stark)
- Ein-Klick-Generator für zufällige, sichere Passwörter
- Kopieren/Einfügen-Knöpfe direkt bei Benutzername und Passwort

BEREICH II

Karten

Die Kamera erkennt Kartennummer, Ablaufdatum und Namen automatisch – auch bei geprägten Karten, deren Ziffern über mehrere Zeilen verteilt sind. Die Erkennung läuft komplett lokal auf dem Gerät, es wird dabei nichts übertragen. Vor dem Speichern lässt sich das Foto noch drehen und die erkannten Werte prüfen.

- Warnt, wenn eine Karte mit bereits vorhandener Nummer erneut gescannt wird
- Eigenes PIN-Feld, unabhängig von der Kartennummer gespeichert
- Kartennummer wird in 4er-Blöcken angezeigt, wie auf der echten Karte

BEREICH III

Datei-Tresor

Der Datei-Tresor ist bewusst vom Rest der App getrennt: eigenes Passwort, eigene AES-256-Verschlüsselung, unabhängig von Face ID. Wer die App per Gesichtserkennung öffnet, kommt ohne dieses zweite Passwort trotzdem nicht an die abgelegten Dateien. Gedacht für Depotunterlagen, Ausweisfotos, Krypto-Seeds oder alles andere, was eine zusätzliche Hürde verdient.

- Bilder aus der Fotothek oder beliebige Dateien aus dem Dateimanager hinzufügen
- Direkte Vorschau per Quick Look, ohne die Datei erst zu exportieren
- Fünf falsche Versuche sperren den Bereich für 5 Minuten und lösen eine Benachrichtigung aus

BEREICH IV

Sicherheit & Backup

Zugang & Sperre

Face ID/Touch ID öffnet die App; wer das lieber ausschaltet, legt stattdessen ein Ersatz-Passwort fest. Eine einstellbare automatische Sperre (1, 5 oder 10 Minuten) schließt Whist zuverlässig, sobald sie im

Hintergrund läuft – auch wenn kein Gerät gesperrt wurde.

Sicherung

Ein Backup lässt sich jederzeit als eigenständig verschlüsselte Datei exportieren – mit einem selbst gewählten Passwort, unabhängig vom App-Zugang. So wandert der Bestand per AirDrop oder Mail sicher vom Mac aufs iPhone oder umgekehrt, ganz ohne automatische Cloud-Synchronisierung.

Was „lokal“ bei Whist bedeutet

Passwörter und Karten liegen im geräteeigenen Schlüsselbund von Apple – demselben geschützten Speicher, den auch iOS und macOS selbst nutzen.

Datei-Tresor und Backup-Export sind zusätzlich mit einem eigenen, aus deinem Passwort abgeleiteten AES-256-Schlüssel verschlüsselt.

Es gibt keinen Whist-Server. Nichts verlässt dein Gerät, außer du exportierst es selbst.

DARSTELLUNG

Anpassbar, aber nicht beliebig

Erscheinungsbild (System/Hell/Dunkel), eine feste Auswahl an Akzentfarben, Textgröße und Fettschrift lassen sich zentral in den Einstellungen anpassen – dazu ein wählbarer Hintergrund aus fertigen Farbverläufen oder einem eigenen Foto. Die Bedienoberfläche selbst ist komplett zweisprachig (Deutsch/Englisch) und wechselt ohne Neustart.

SYSTEMVORAUSSETZUNGEN

Geräte & Plattformen

Gerät	Face ID / Touch ID	Anmerkung
Mac	Touch ID, wo vorhanden	eigenständige App, kein Browser nötig
iPhone	Face ID / Touch ID	Kamera-Scan für Karten benötigt Kamerazugriff
iPad	Face ID / Touch ID	gleiche Funktionen wie auf dem iPhone