

VasukisHold

USER GUIDE

Your offline, encrypted vault for passwords, bank details, company records, cards and personal ledgers.

Version 2.0 · Works offline on Windows, Mac, Linux & Android
Sold by nomadicmirage.com

WELCOME

Before you begin

VasukisHold keeps your most sensitive information in one encrypted file that only you can open. There is no account, no cloud and no internet connection. This guide takes you from your first vault to everyday use, backups and good security habits.

1 file
The app runs in your browser; nothing to install.

2 locks
A master password *and* a keyfile. Neither works alone.

0 internet
VasukisHold is blocked from connecting anywhere.

Contents

1 The book, the safe and the key — how VasukisHold works3

2 What you need & where to keep each file4

3 Create your vault5

4 Unlock your vault6

5 A tour of the app7

6 Logins, passwords & 2FA codes8

7 Companies, bank accounts & cards9

8 The ledger: money given & received10

9 Upcoming: reminders & expiry dates11

10 Importing data from spreadsheets12

11 Saving & backups13

12 Security habits & settings14

13 What if…? Troubleshooting15

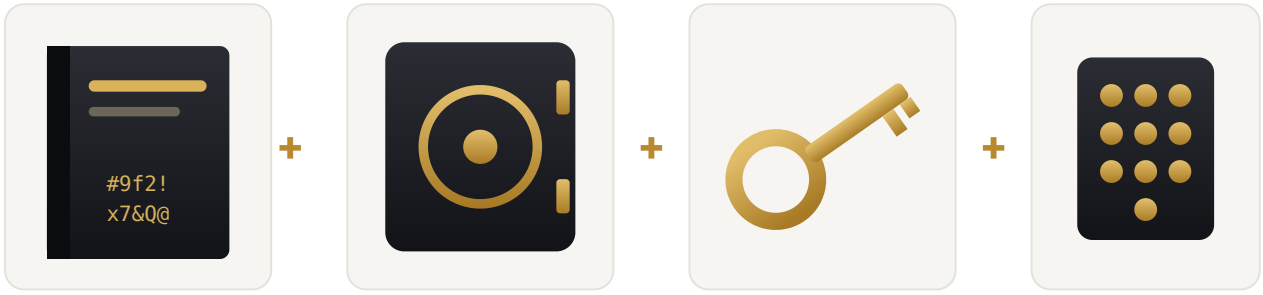
14 FAQ & quick reference16

The one rule that matters most: nobody can recover a lost master password or keyfile — not you, not the seller, not anyone. Keep a backup keyfile and a written copy of your password somewhere safe *before* you store real data.

CHAPTER 1

The book, the safe and the key

VasukisHold works like something people have trusted for centuries: a ledger kept in a safe, opened with a key and a combination.



THE LEDGER `vault.dat`

THE SAFE `VasukisHold.html`

THE KEY `vault.key`

COMBINATION master password

Book + Safe + Key + Combination = your data, readable

📖 The Ledger — `vault.dat`

Your book. Every password, account and record lives here, written entirely in code. Open it in any other program and it's meaningless characters. That's why you can carry it on a pendrive safely.

🗄️ The Safe — `VasukisHold.html`

The only thing that turns the coded book back into readable pages. It holds no secrets of its own, so it's **replaceable**: lose it, download it again, and your book still opens.

🔑 The Key — `vault.key`

A small file of 512 random bits, created once. Keep it **separate from the book** — for example on your phone while the book lives on your pendrive.

🔢 The Combination — your password

Carried only in your head. Even someone with both your book and your key still needs it, and every guess costs them seconds and half a gigabyte of memory.

> **Losing any single piece exposes nothing.** A stranger needs the book, the key *and* the combination together.

CHAPTER 2

What you need & where to keep each file

Supported devices

DEVICE	BROWSER	EXPERIENCE
Windows, Mac, Linux	**Chrome** or **Edge**	✅ Best — saves straight back to your pendrive automatically
Android phone / tablet	**Chrome**	✅ Full support, from phone storage or a pendrive via OTG cable
Any device	Firefox, Safari, others	⚠️ Opens, but saving works by *downloading* a new copy that you then move into place
iPhone / iPad	—	⚠️ Limited; not recommended

Always open `VasukisHold.html` in the browser itself — not in a file manager's "preview". If the welcome screen shows a red box saying something is missing, open the file in Chrome.

Where to keep each file



PENDRIVE

`VasukisHold.html`
`vault.dat`



YOUR PHONE

`vault.key`
(protected by screen lock)



AT HOME

backup copy of vault.key
backup copy of vault.dat
password written on paper

Never keep vault.key on the same pendrive as vault.dat

Why separate?

If someone finds your pendrive, they get the book — but not the key. If someone takes your phone, they get the key — but not the book. Both must be lost together, *and* the password guessed, before anything is exposed.

Choosing a good password

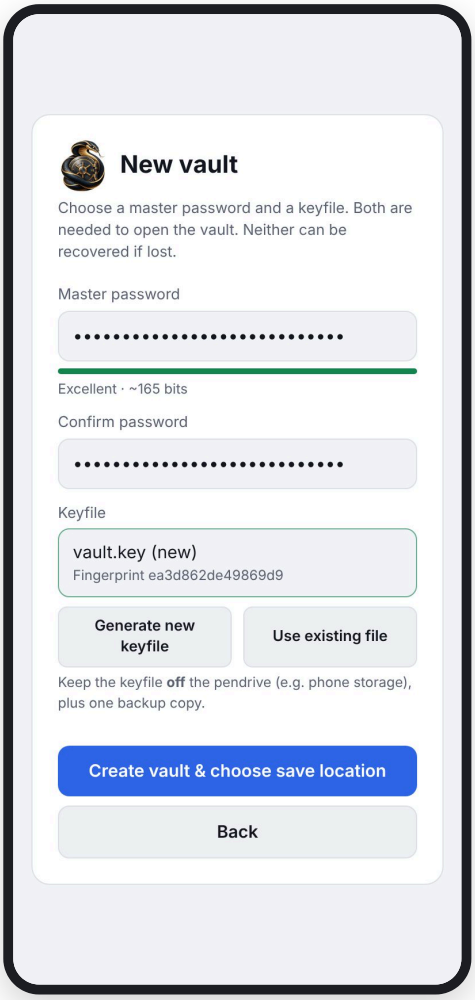
At least 12 characters. Best: **5–6 random words**, e.g. `river lamp mango tiger ocean`. Easy to remember, very hard to guess. Never reuse a password from another site.

CHAPTER 3

Create your vault

You do this once. It takes about two minutes.

1. **Copy the app to your pendrive**
   Put `VasukisHold.html` on the pendrive (or any folder you'll use).
2. **Open it in Chrome or Edge**
   On a computer, double-click it (or right-click → Open with → Chrome). On Android, use your file manager → *Open with* → **Chrome**.
3. **Tap "Create new vault"**
4. **Choose your master password**
   Type it twice. The bar shows its strength — aim for **Strong** or **Excellent**.
5. **Tap "Generate new keyfile"**
   Save `vault.key` to your **phone storage or PC** — not the pendrive. Note the *fingerprint* shown; it identifies this exact keyfile.
6. **Tap "Create vault & choose save location"**
   Save `vault.dat` to your **pendrive**. Unlocking takes about 4 seconds while your key is prepared.
7. **Make your backups now**
   Copy `vault.key` to a second place (e.g. a USB kept at home) and write your password on paper for your home safe.



The "New vault" screen with password and keyfile ready

> **Already have a keyfile?** Tap *Use existing file* instead of generating one. Any file of 32 bytes or more can be a keyfile — but a generated one is best.

CHAPTER 4

Unlock your vault

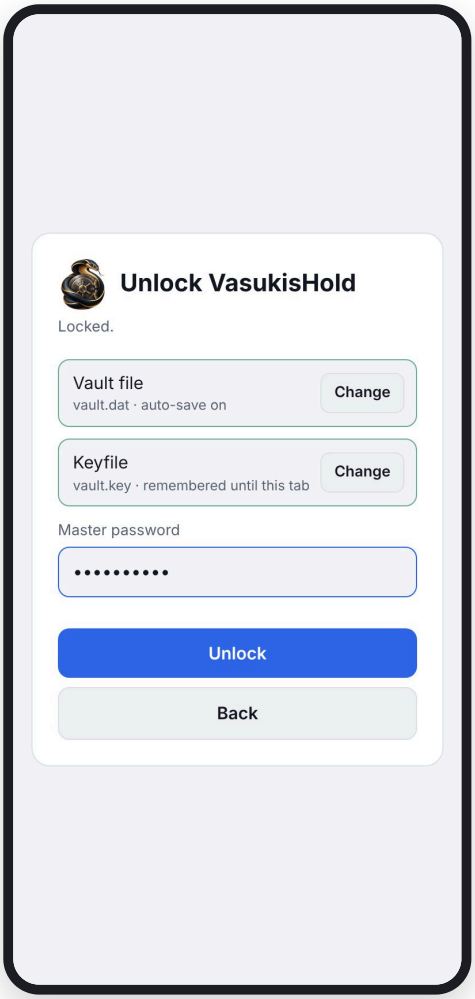
Every time you want to use VasukisHold, bring the three pieces together.



1. **Open `VasukisHold.html` and tap "Open existing vault"**
2. **Vault file → Choose**
   Pick `vault.dat` from your pendrive. On Chrome/Edge this also turns on **auto-save**.
3. **Keyfile → Choose**
   Pick `vault.key` from your phone or PC.
4. **Type your master password and tap Unlock**

> **Re-unlocking is quicker.** After a lock, VasukisHold remembers which vault and keyfile you chose until you close the browser tab — just type the password again.

> **"Wrong password or keyfile."** Check Caps Lock, and make sure you picked the right keyfile (compare its fingerprint in *Settings*). The vault can't tell you which of the two is wrong — that's deliberate.

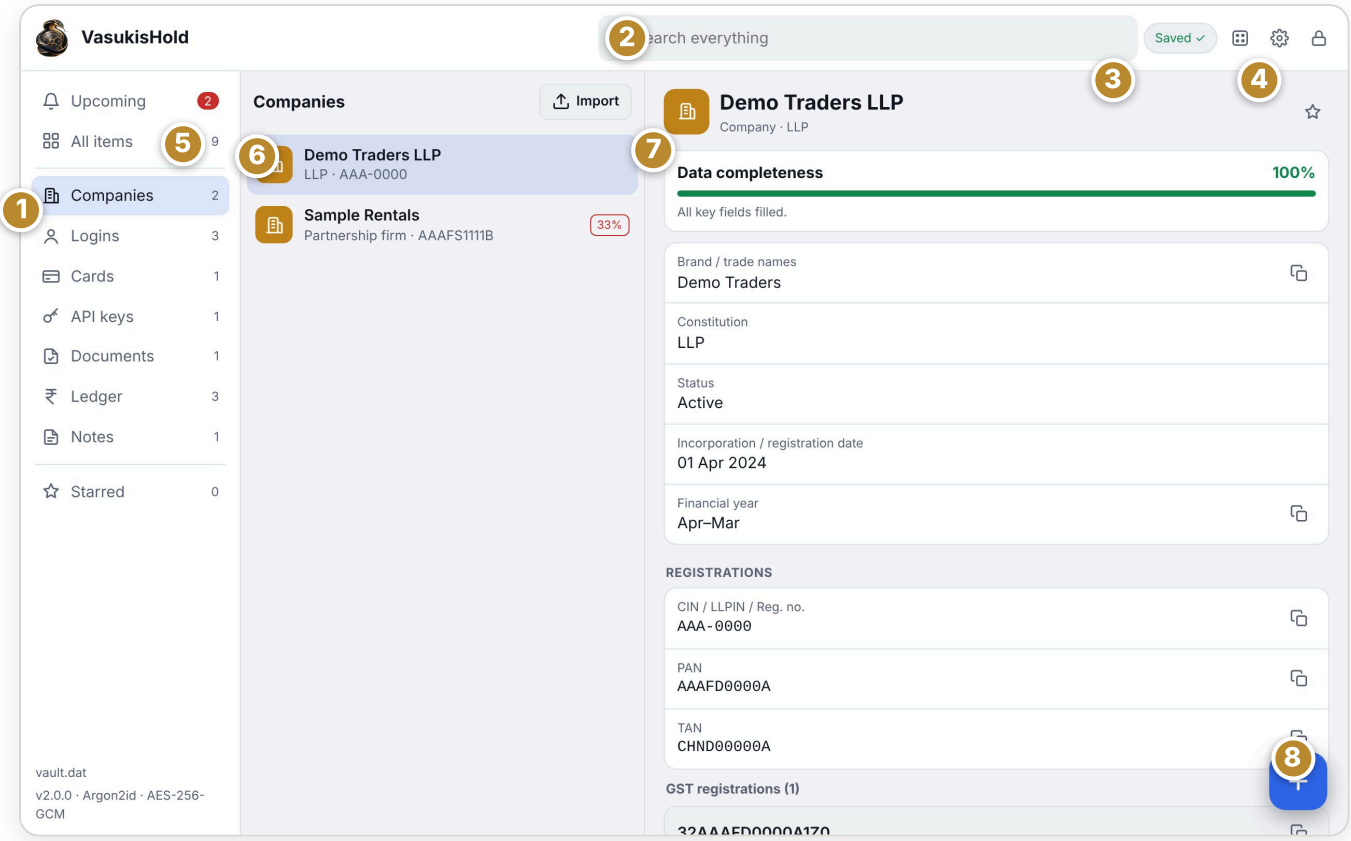


Vault file and keyfile chosen — just the password left

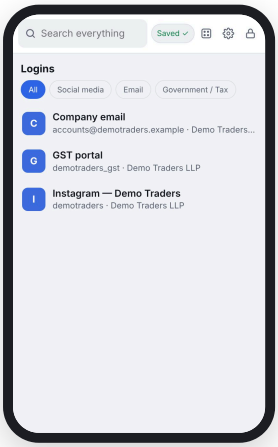
CHAPTER 5

A tour of the app

On a computer you see three panes; on a phone, one at a time with tabs at the bottom.



1. **Sections** — Upcoming, All items, Companies, Logins, Cards, API keys, Documents, Ledger, Notes, Starred.
2. **Search everything** — names, usernames, GSTINs, notes… (hidden secrets are never searched).
3. **Save status** — Saved ✓ means your pendrive copy is up to date. Tap it to save manually.
4. **Tools** — password generator, settings & import, and **Lock**.
5. **Item count** per section; a red badge on Upcoming means something is due within 7 days.
6. **List** — tap any row. Badges show expiry, completeness or amounts.
7. **Details** — copy buttons, show/hide eye, Edit and Delete at the bottom.
8. **+ button** — add a new item to the current section.

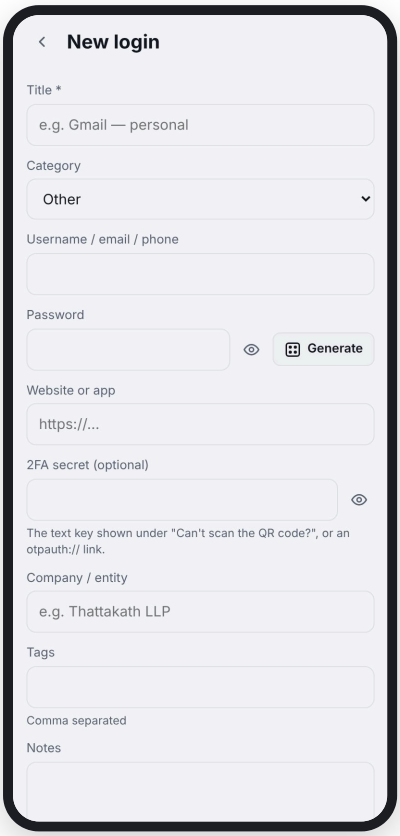


On a phone: the bottom bar has **Upcoming, Companies, Logins, Ledger** and **More** (Cards, API keys, Documents, Notes, Starred). Tap an item to open it; use the ‹ arrow to go back.

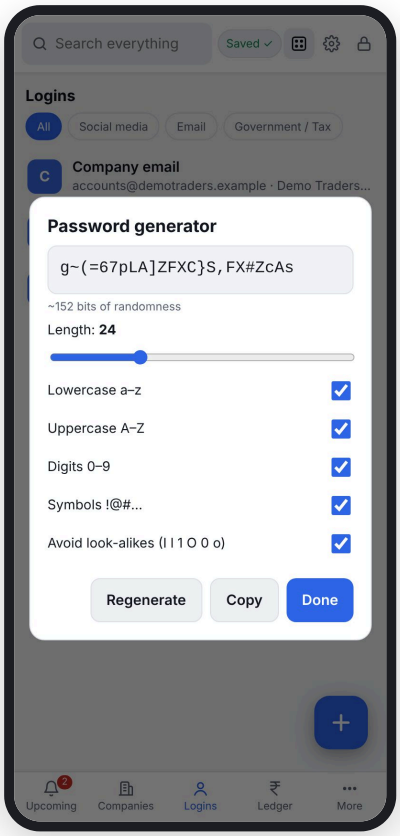
Shortcuts on a computer: press `Esc` `Esc` quickly or `Alt`+`L` to lock instantly.

CHAPTER 6

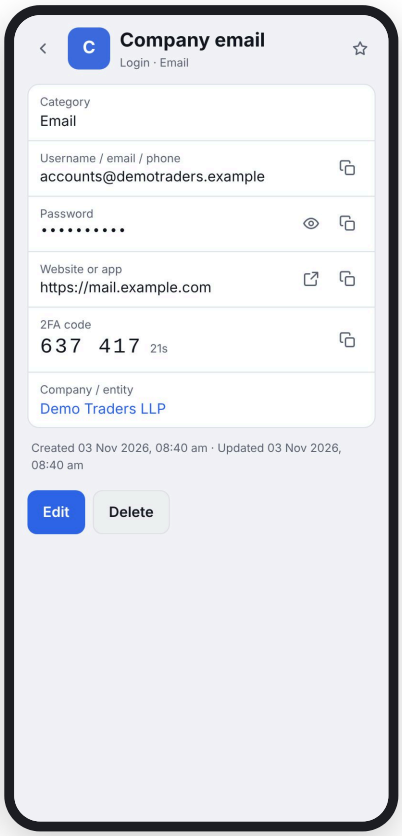
Logins, passwords & 2FA codes



Adding a login



Password generator



Live 2FA code

Add a login

1. **Logins → +**
   Give it a clear title, e.g. *Gmail — personal*, and pick a category.
2. **Username and password**
   Tap Generate for a strong new password, then **Use**.
3. **Optional extras**
   Website, company, tags, notes and a 2FA secret. Tap **Save**.

Two-factor (2FA) codes

When a website shows a QR code to set up 2FA, tap *"Can't scan the QR code?"* and copy the text key it shows. Paste it into **2FA secret**. VasukisHold now shows the 6-digit code, refreshing every 30 seconds — no separate authenticator app needed.

Copying safely

Tap the copy icon next to any field. Copied text is **cleared from the clipboard after 20 seconds**. Passwords stay hidden until you tap the 👁 eye.

Password history

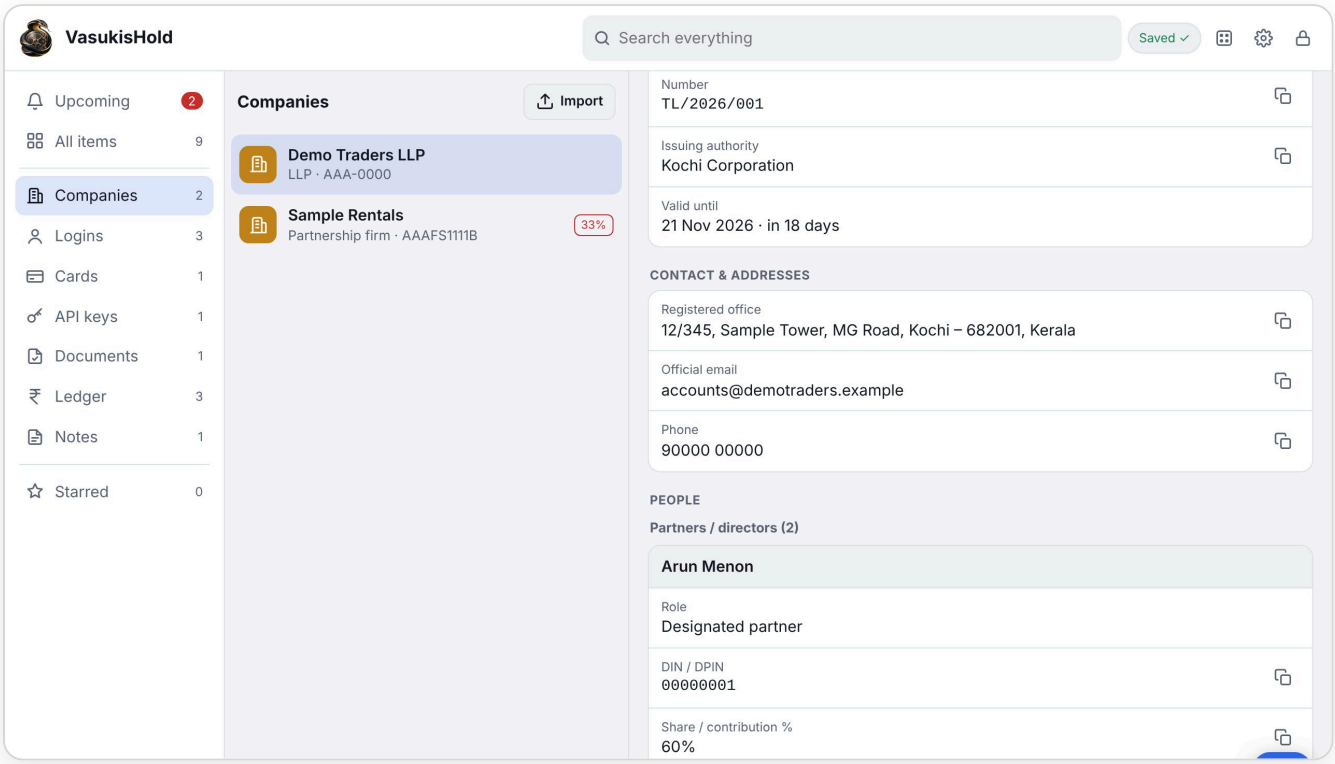
When you change a password, the old one is kept under *Previous passwords* (last 5) — handy if a change didn't go through.

> **Phone keyboards remember copied text.** Gboard and Samsung Keyboard keep a clipboard history that VasukisHold can't clear. Turn off clipboard history in your keyboard settings, or delete copied passwords from it.

CHAPTER 7

Companies, bank accounts & cards

One profile per firm, LLP, company or proprietorship — with everything in one place.



A company profile: registrations, contact details, partners and bank accounts

What a company profile holds

- **Registrations:** CIN / LLPIN / firm no., PAN, TAN, Udyam, IEC, GSTINs
- **Licences** with issuing authority and **expiry date**
- **Partners / directors** with role, DIN, PAN and share
- **Bank accounts:** number (hidden until tapped), IFSC, MICR, signatories, mode of operation, linked net-banking login
- Branch addresses, CA / CS / lawyer contacts, **compliance calendar**, custom fields

Data completeness

Each company shows a score and a **"Missing:"** list — e.g. *TAN, Bank ••5353: signatories*. Fill those in and it reaches 100%.

Adding a bank account

Open the company → **Edit** → scroll to **BANKING** → **+ Add bank account** → **Save**. (Empty sections only appear in Edit mode.)

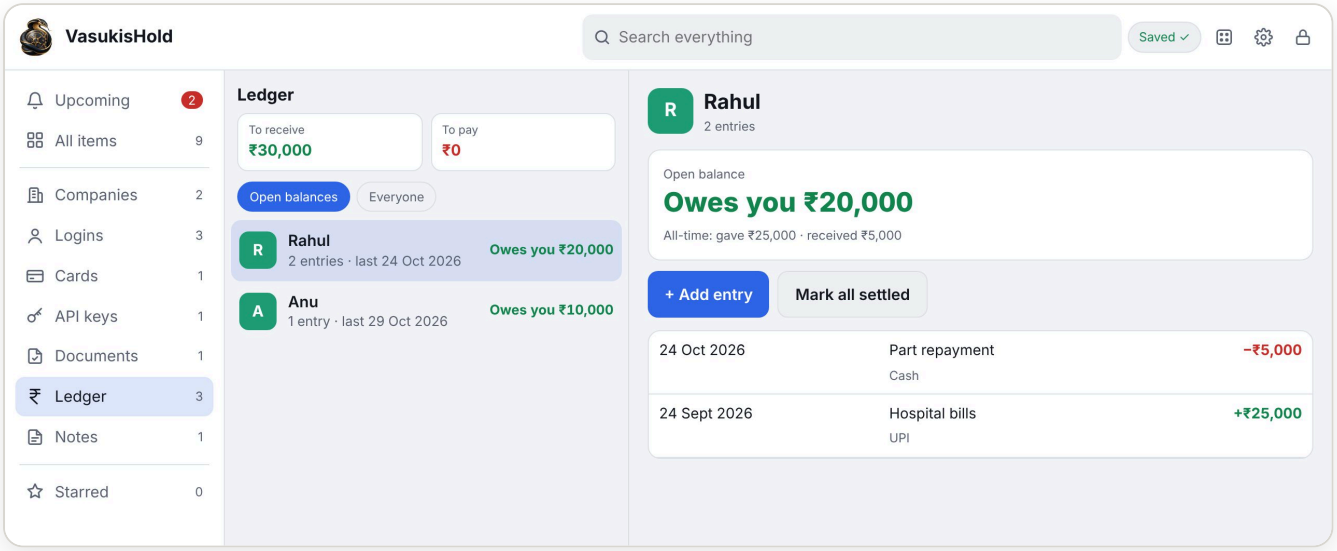
Cards

In **Cards**, store card type, bank, expiry (MM/YY), limit and **payment due day**. Card number, CVV and PIN are masked; the list only ever shows the last 4 digits.

CHAPTER 8

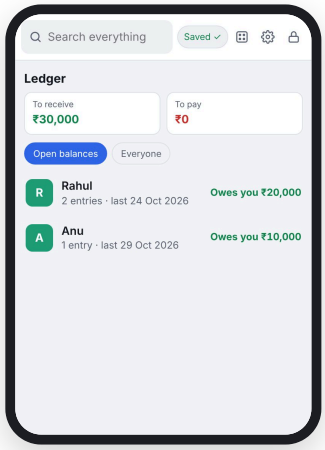
The ledger: money given & received

Keep an exact record of money you lend to or receive from friends and family — in rupees, with running balances.



One person's history: open balance, every entry, and "Mark all settled"

Record an entry



1. **Ledger → +**
   Type the person's name (previous names are suggested).
2. **Direction**
   I gave money (they owe you) or *I received money* (repayment, or you owe them).
3. **Amount, date, mode**
   UPI, cash, bank transfer… add the UTR/reference and purpose.
4. **Optional "Repay by" date**
   It appears in Upcoming as a reminder.

Owes you ₹20,000
They have money of yours.

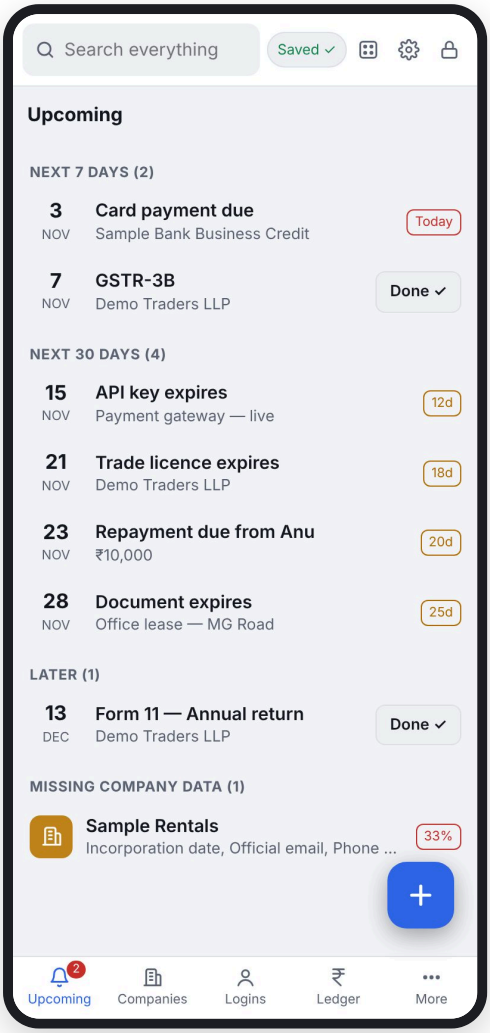
You owe ₹5,000
You have money of theirs.

Settled
Tap *Mark all settled* once squared up — history stays.

CHAPTER 9

Upcoming: reminders & expiry dates

VasukisHold opens on **Upcoming** — one list of everything that needs your attention.



What appears here

SOURCE	DATE USED
Company licences	Valid until
Compliance calendar	Next due
Documents	Expires on, renewal date
API keys	Expires on
Cards	Payment due day, card expiry
Ledger	Repay by (unsettled only)

Groups

Overdue · Next 7 days · Next 30 days · Later — plus **Missing company data** at the bottom.

"Done ✓" for repeating tasks

Compliance items such as *GSTR-3B (Monthly)* or *Form 11 (Yearly)* have a **Done ✓** button. Tap it and the next due date is set automatically.

How far ahead?

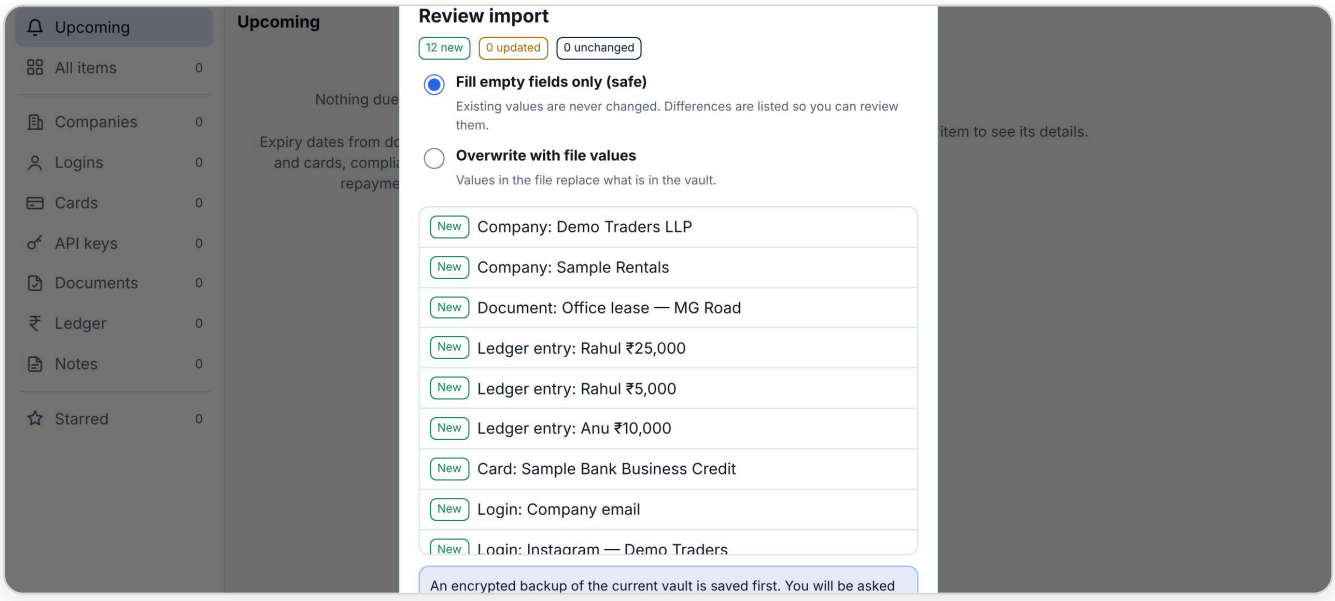
By default, 60 days. Change it in **Settings → Show upcoming dates within** (30, 60, 90 or 180 days).

CHAPTER 10

Importing data from spreadsheets

Have years of records in Excel or Google Sheets? Bring them in all at once.

1. **Settings ⚙ → Import data (JSON / CSV)**
   Or the **Import** button in Companies.
2. **Download a template**
   Open *Templates* and download the CSV you need — companies, bank accounts, GST, licences, partners, documents, ledger, cards, logins...
3. **Fill it in Excel / Sheets**
   Dates as `DD-MM-YYYY` or `YYYY-MM-DD`; amounts like `1,20,000` are fine. Save as CSV.
4. **Choose files → Preview**
   Pick one or more files at once. Child files (banks, GST, partners) link to a company by its **name, CIN or PAN**.
5. **Review, then "Back up & import"**
   An encrypted backup of your vault is saved first.
6. **Delete the CSV/JSON files**
   They are **not encrypted**.



The import preview — nothing changes until you confirm

Fill empty fields only (safe) — never changes what you already have; differences are listed for you to review.
Overwrite — values in the file replace what's in the vault.

Never imported, by design: passwords, PINs, CVVs, API keys and secrets, 2FA secrets and full card numbers. Type those in by hand. Importing the same file twice won't create duplicates.

CHAPTER 11

Saving & backups

Reading the save button

YOU SEE	MEANING	WHAT TO DO
Saved ✓	Your `vault.dat` is up to date.	Nothing.
Saving…	Writing to your pendrive (under a second).	Don't unplug the pendrive.
Tap to save	Auto-save isn't connected for this file.	Tap it and choose your existing `vault.dat` to overwrite.
Tap to download	Your browser can't save directly.	Tap it, then replace the old `vault.dat` with the downloaded copy.
⚠ Tap to save	The last save failed (e.g. pendrive removed).	Reconnect, then tap to save.

The 3-2-1 backup habit



Making a backup
Copy `vault.dat` to another drive like any file — or use **Settings → Save encrypted backup**. Backups are encrypted with the same password and keyfile, so they're just as safe. Refresh them after big changes.

Import backups
Each import saves `vault-before-import-DATE.dat` — an undo copy. **Keep the suggested name; never save it over `vault.dat`.** Once you've checked the import, you can delete it.

> **Updating VasukisHold:** replace the old `VasukisHold.html` with the new one — your vault upgrades automatically. Back up `vault.dat` first: after an upgrade, older app versions can no longer open it.

CHAPTER 12

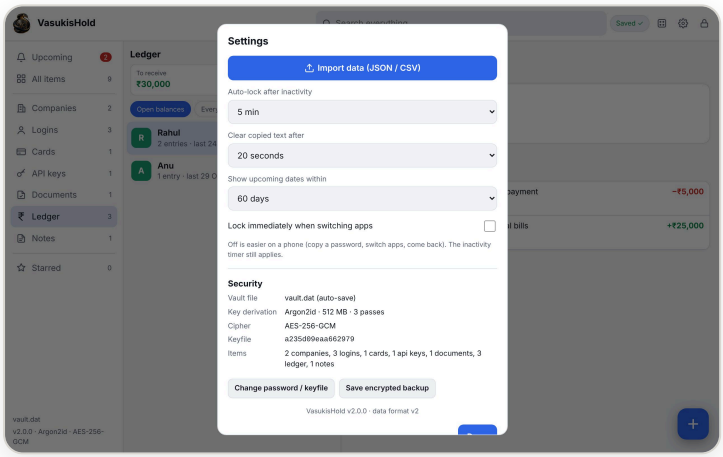
Security habits & settings

DO

- ✔ Use a 5–6 random-word master password
- ✔ Keep the keyfile and the vault on different devices
- ✔ Keep 2 keyfile copies and 3 vault copies
- ✔ Unlock only on your own, trusted devices
- ✔ Lock when you step away (`Esc` `Esc`)
- ✔ Delete import files after using them
- ✔ Keep a trusted copy of `VasukisHold.html` on your PC

DON'T

- ✕ Unlock on office, shared or cyber-café computers
- ✕ Store `vault.key` on the same pendrive as `vault.dat`
- ✕ Email, WhatsApp or upload your keyfile
- ✕ Reuse your master password anywhere else
- ✕ Leave the vault unlocked on a shared screen
- ✕ Trust a pendrive that's been out of your hands — replace its `VasukisHold.html` with your trusted copy



Settings ⚙

- **Auto-lock after inactivity:** 1–30 min (default 5)
- **Clear copied text after:** 10–90 sec (default 20)
- **Lock when switching apps:** strongest on phones; off by default for convenience
- **Change password / keyfile:** re-encrypts the vault. *Old backups still open with the old ones — replace them.*
- **Save encrypted backup**
- **Keyfile fingerprint:** to confirm which keyfile is which

Under the hood: AES-256-GCM encryption; Argon2id key stretching (512 MB, 3 passes); master password + keyfile combined; tamper detection; no network access. No software can protect a device that already has malware or a keylogger.

CHAPTER 13

What if…? Troubleshooting

SITUATION	WHAT TO DO
I lost my pendrive	Your data is unreadable to whoever finds it. Restore `vault.dat` and `VasukisHold.html` from your backups. For extra safety, use *Change password / keyfile* afterwards.
I lost my phone (with the keyfile)	Use your backup keyfile. Then *Change password / keyfile*Generate a new keyfile, and update all backups.
I lost `VasukisHold.html`	No problem — get a fresh copy. Your vault opens exactly as before.
I forgot my password / lost every keyfile	The vault cannot be opened by anyone. There is no reset. This is why backups and the paper copy matter.
"Wrong password or keyfile"	Check Caps Lock and keyboard language. Confirm the keyfile's fingerprint matches the one in Settings (or your notes).
Red box: "This browser is missing..."	You're in a file preview or an old browser. Open the file in Chrome or Edge.
"This is not a vault file"	You picked the wrong file (e.g. the keyfile as the vault). Choose `vault.dat`.
"Saved by a newer version of the app"	Use the newest `VasukisHold.html`.
Status stays "Tap to save"	Tap it and choose your existing `vault.dat`; or unlock by picking the vault through *Choose* so auto-save is connected.
Phone: changes not on the pendrive	Make sure the pendrive is still connected and the status shows Saved ✓ before unplugging.
Locked in the middle of work	Auto-lock kicked in. Any unsaved changes are kept (encrypted) — unlock again to continue. Increase the time in Settings if needed.
An import went wrong	Unlock the `vault-before-import-…dat` backup instead, then *Save encrypted backup* over `vault.dat`.
A bank account section is missing	Empty sections show only in **Edit**. Open the company → Edit → BANKING → + Add bank account.

CHAPTER 14

FAQ & quick reference

Does VasukisHold use the internet?
Never. It is blocked from connecting anywhere. Tapping a saved website link simply opens that site in a separate tab.

Can the seller see my data?
No. Your data never leaves your device.

Can I store scanned documents?
No — VasukisHold is text-only by design, which keeps it small and fast. Use the Document register to record where each original is kept.

Can I use one vault on my PC and phone?
Yes — it's the same file. Carry it on the pendrive, or copy it across; just make sure you always work on the newest copy.

Can two people share a vault?
Only by sharing the file, keyfile and password — which shares everything. Separate vaults are better.

What does the keyfile fingerprint do?
It's a short ID for your keyfile, safe to write down, so you can confirm two copies are identical.

QUICK REFERENCE CARD

Open	VasukisHold.html in Chrome / Edge
Unlock	vault.dat + vault.key + password
Lock	🔒 button · Esc Esc · Alt+L
Add	+ button in any section
Find	Search everything (top bar)
Generate	🎲 password generator
Import	⚙ Settings → Import data
Backup	⚙ Settings → Save encrypted backup
Saved?	Status shows "Saved ✓"
Remember	Keyfile never on the vault's pendrive

My keyfile record (fill in by hand)

Fingerprint: _____

Keyfile copy 1 kept at: _____

Keyfile copy 2 kept at: _____

Vault backups kept at: _____

> Purchased from **nomadicmirage.com**. VasukisHold is a digital product and is non-refundable — see the Terms & Conditions on the website. For help, contact **[support email]**.