MI8OS

INSIDE MI8OS · MOBILE EDITION

Everything about your app and your cards.

How to create, open and update a vault, how to look after your MI8OS Card gen 2, and exactly how your secrets are protected, down to the last byte.

CREATE · USE · CARDS · SECURITY



Scroll to start · iPhone and Android · October 2026

CONTENTS · TAP TO JUMP

What's inside

01 **GETTING STARTED**
What MI8OS is, the words you'll meet, the app at a glance, how to hold a card. →

02 **CREATE A VAULT**
Add secrets, choose a Vault Password, save to a card, write your backup cards. →

03 **USE YOUR VAULT**
Open a card, read and copy secrets, 2FA codes, add and delete, update the card. →

04 **MANAGE YOUR CARDS**
My Cards, rename, identify, reset, lock and unlock with a Master Password. →

05 **SETTINGS**
App Lock, Face ID, the clipboard and appearance. →

06 **HOW YOUR SECRETS ARE PROTECTED**
Two layers of encryption, a real example with "12345678", and why your Vault Password matters. →

07 **CARE, ANDROID AND HELP**
Keeping three cards, Android differences, troubleshooting. →

Reading on a computer or want to print? There's an A4 edition with the same content.

01

Getting started

Five minutes to understand how MI8OS works, before you touch a card.

01 What MI8OS is
02 Words you'll meet
03 The app at a glance
04 Holding the card
05 What belongs on a card

WHAT MI8OS IS

A small, encrypted vault on a card you hold.

MI8OS keeps your most important secrets, like recovery codes, 2FA keys, seed words and PINs, in a vault that is encrypted on your phone and saved to a physical card. No account, no cloud, no subscription.



Carry · the one you use



Home · safe at home



Elsewhere · somewhere else

WHAT MI8OS IS

IN YOUR SET

Three **MI8OS Cards, gen 2**. Each card holds up to **20 secrets**. Write the same vault to all three and keep them in different places.

WHAT YOU NEED

An iPhone or Android phone with NFC and the MI8OS app from the App Store or Google Play (Android notes). And a Vault Password you can remember: a long passphrase is best.

WORDS YOU'LL MEET

Three passwords, three different jobs.

This is the most important page in this guide. They sound alike, but each one protects something different.

VAULT PASSWORD

Encrypts and opens the secrets on a card. Required, at least 12 characters.

Never stored anywhere. Nobody can recover it, not even MI8OS.

WORDS YOU'LL MEET

MASTER PASSWORD

Optional. Locks the card itself, so nobody can reset or erase it without this password.

Opens nothing. Reading secrets still needs the Vault Password.

APP LOCK PIN

Optional. Six digits (or Face ID) to open the app on this phone.

Has nothing to do with your cards and can't decrypt anything.

WORDS YOU'LL MEET

Vault
Your list of secrets. It exists encrypted on your cards, and decrypted only in the app's memory while it's open.

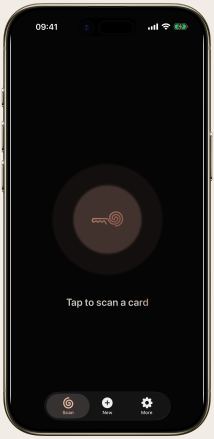
Secret
One entry: a name (up to 24 bytes) and the secret itself (up to 96 bytes), such as a PIN, a recovery code or a 2FA key.

Card
Your MI8OS Card gen 2. It stores the encrypted vault; you can write the same vault to several cards.

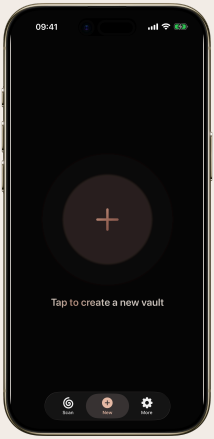
Update Card
Writes your changes to the card. Until then, changes live only in the app's memory.

THE APP AT A GLANCE

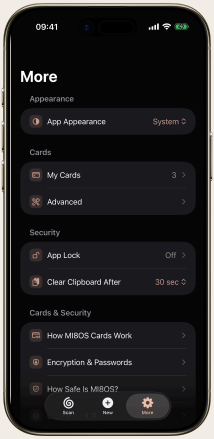
Three tabs. One job each.



Scan · open a card



New · create a vault



More · cards and settings

THE APP AT A GLANCE

1 **SCAN**

Tap to scan a card and hold your card to the phone. The card opens in its own window, where you enter its Vault Password.

2 **NEW**

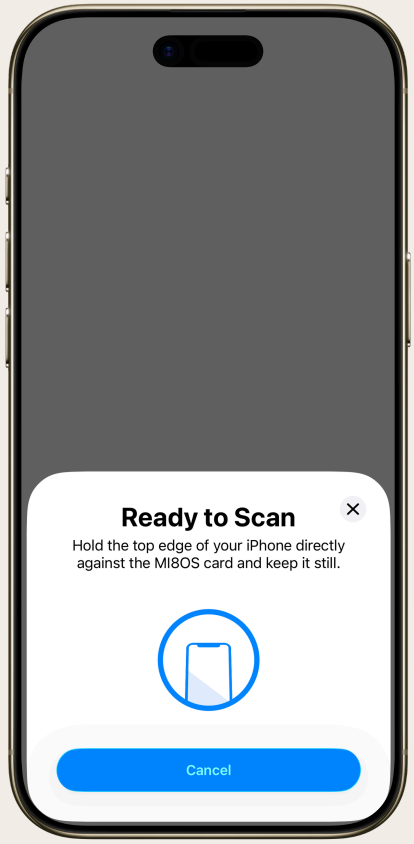
Tap to create a new vault. A four-step guide takes you from your first secret to a card that holds it.

3 **MORE**

Your cards, App Lock, the clipboard timer, appearance and the built-in help pages.

HOLDING THE CARD

Top edge. Flat. Still.



HOLDING THE CARD

Every time the app talks to a card, iPhone shows its own NFC prompt. Then:

1. **Hold the card flat against the top edge** of the back of your iPhone, where the NFC antenna sits.
2. **Keep it still** until the app confirms. Writing takes a few seconds; moving the card early is the most common reason a write needs to be repeated.
3. If nothing happens, slide the card slowly a little lower or higher, and remove thick or metal cases.

> **No need to rush.** When you open a card, the app first prepares your key ("Preparing your key. No need to hold the card yet"). Hold the card when the NFC prompt appears.

> **On Android**, the app shows its own scan screen and the card goes against the upper half of the back of the phone.

WHAT BELONGS ON A CARD

A few secrets that matter a lot.

MI8OS isn't meant to replace your password manager. It's the offline place for the handful of things you'd need if everything else failed.

GREAT ON A CARD

- ✓ Recovery codes for email and Apple / Google
- ✓ 2FA setup keys, so the app can show your codes
- ✓ Crypto recovery phrases (MI8OS isn't a wallet and holds no funds)
- ✓ Your password manager's master password or emergency kit details
- ✓ Important PINs and private notes

WHAT BELONGS ON A CARD

GOOD TO KNOW

- ✓ Up to 20 secrets per card
- ✓ Name: up to 24 bytes · secret: up to 96 bytes
- ✓ Plain letters, digits and spaces use 1 byte; accented, Greek or Cyrillic letters 2; emoji 4
- ✓ Long seed phrases may need two secrets (e.g. words 1–12 and 13–24)

02

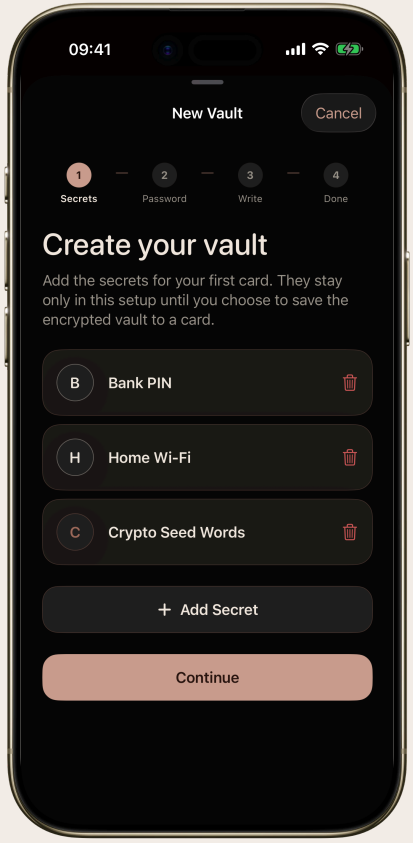
Create a vault

Four steps: Secrets, Password, Write, Done. About five minutes.

01 Step 1 of 4 · Secrets
02 Step 2 of 4 · Password
03 Step 3 of 4 · Write
04 Step 4 of 4 · Done
05 A card that already has a vault

STEP 1 OF 4 · SECRETS

Start with your secrets.



STEP 1 OF 4 · SECRETS

1. Open the **New** tab and tap the **Tap to create a new vault** button.
2. Tap **Add Secret** for each thing you want to keep.
3. Swipe a secret to remove it again before you continue.
4. Tap **Continue** when your list is ready.

> **Nothing is saved yet.** Your secrets stay only in this setup until you save the encrypted vault to a card.

> **Already have a vault open?** The app asks first. If you have changes that aren't on a card yet, it offers to keep them.

ADDING A SECRET

A name, and the secret itself.



ADDING A SECRET

Name. Something you'll recognise, like "Email recovery codes". Up to 24 bytes; a counter shows how much is left.

Secret. The password, code or text, up to 96 bytes. Anything you paste or generate is encrypted before it reaches a card.

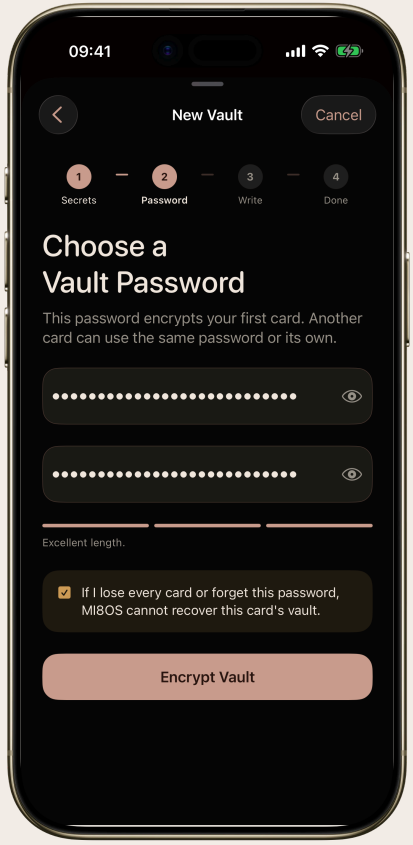
Generate. Tap the dice to create a random password of 16, 32, 64 or 96 characters.

SAVING A 2FA KEY

When a service shows the setup key (or the **otpauth://** link behind its QR code), paste it as a secret. MI8OS recognises it and later shows a **TOTP** button that copies the current code. If the link is longer than 96 bytes, paste only the setup key itself (the part after **secret=**); MI8OS then uses the standard 6 digits every 30 seconds.

STEP 2 OF 4 · PASSWORD

Choose your Vault Password.



STEP 2 OF 4 · PASSWORD

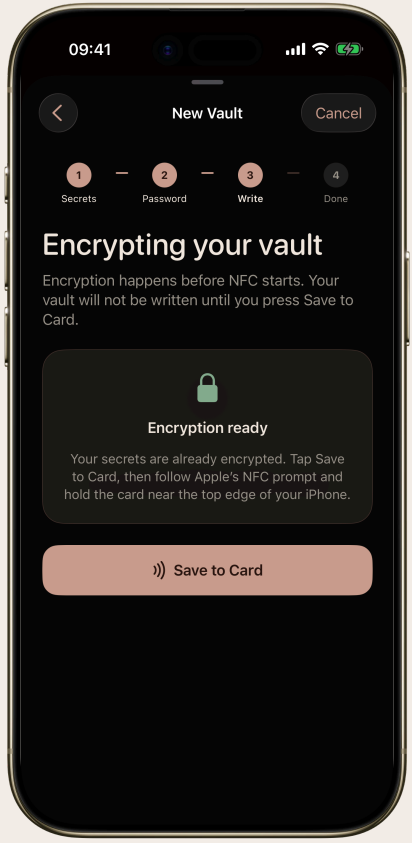
1. Type your Vault Password, then type it again to confirm.
2. Watch the strength bar: 12 characters is the minimum, 20 or a phrase with spaces is "Excellent length."
3. Tick the box: *"If I lose every card or forget this password, MI8OS cannot recover this card's vault."*
4. Tap **Encrypt Vault**.

OUR ADVICE

Use **five or six random words**, like *copper lantern velvet orbit tundra* (but not this one). Easy to remember, extremely hard to guess. See why.

STEP 3 OF 4 · WRITE

Encrypt first. Then tap.



STEP 3 OF 4 · WRITE

Encryption happens on your phone, before NFC starts. You'll see "Strengthening your encryption..." for a moment while the app turns your password into keys. That pause is deliberate: it makes guessing your password slow for anyone else.

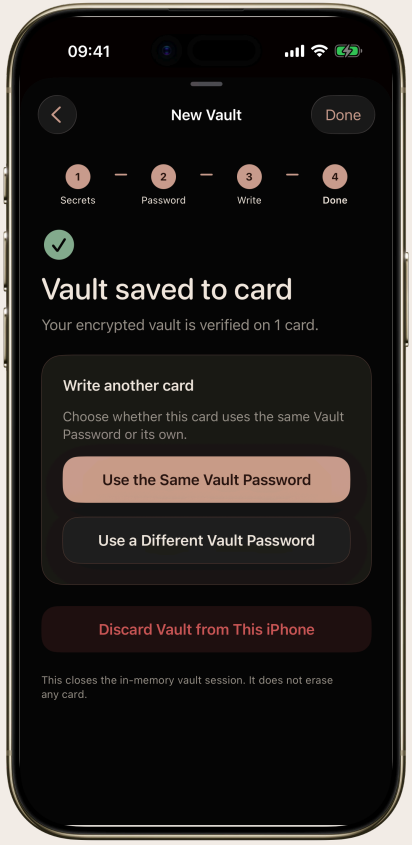
When it says **Encryption ready**:

1. Tap **Save to Card**.
2. Hold your card to the top edge of the iPhone when the NFC prompt appears.
3. Keep still. The app writes the vault, then **reads it back to check it**.

> **Blank card?** The app prepares it automatically in the same tap.

STEP 4 OF 4 · DONE

Now write your backup cards.



STEP 4 OF 4 · DONE

"Vault saved to card" means the vault is verified on that card. **This is the only moment the app can copy your whole vault to other cards**, so write all of them now:

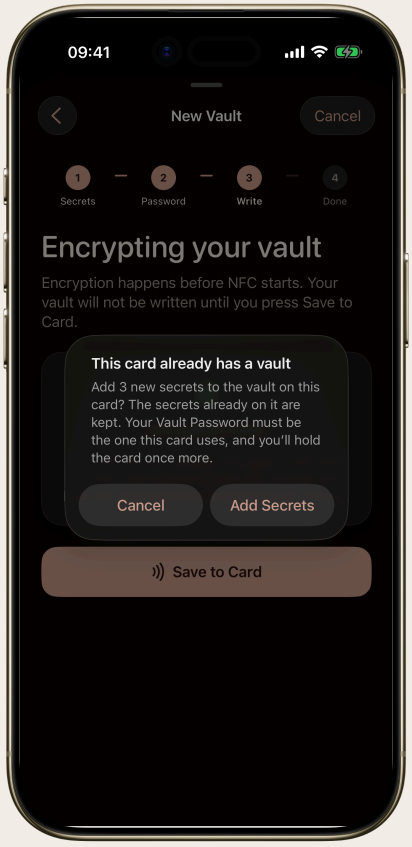
1. Tap **Write Another Card**.
2. Choose **Use the Same Vault Password** (simplest) or **Use a Different Vault Password** for this card.
3. Save to the next card. Repeat for the third.

> **Same password, new encryption.** Each card gets its own random salt, so even with the same password, every card's data looks completely different.

Discard Vault from This iPhone only closes the vault in the app's memory. It never erases a card.

A CARD THAT ALREADY HAS A VAULT

MI8OS never overwrites a vault by surprise.



A CARD THAT ALREADY HAS A VAULT

If you save a new vault to a card that already holds one, nothing is written. The app tells you: **"This card already has a vault"**, and gives you two choices:

ADD SECRETS

Adds your new secrets to the vault on the card. The secrets already on it are kept. Your Vault Password must be the one this card uses, and you hold the card once more.

CANCEL

Leaves the card exactly as it was.

> **Want to replace the vault completely?** Reset the card first, then create the new vault on it.

03

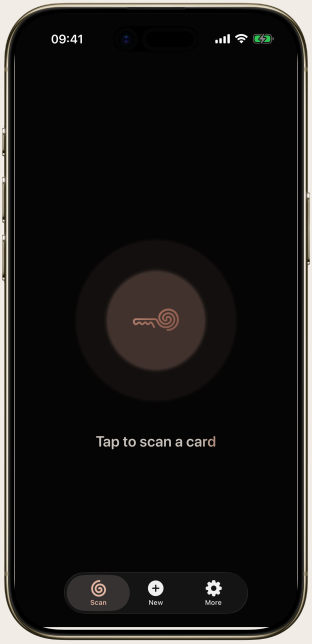
Use your vault

Open, read, copy, change, and write the changes back to the card.

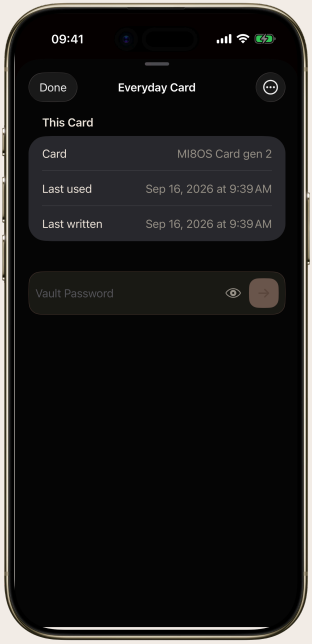
01 Open a card
02 Inside the vault
03 Read and copy
04 2FA codes
05 Change the vault
06 Keep every copy current

OPEN A CARD

Scan, password, hold again.



Scan tab



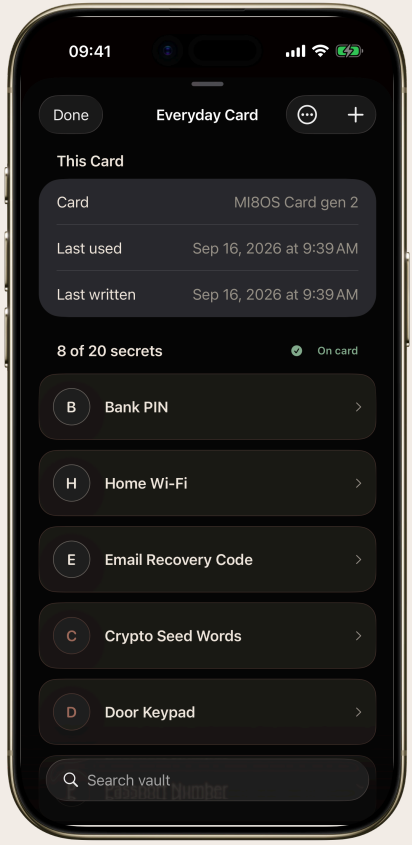
The card's window

OPEN A CARD

1. On **Scan**, tap the **Tap to scan a card** button and hold the card. Scanning only reads the card's public information.
2. Enter the card's **Vault Password** and tap **Open Vault**. The app prepares your key, then asks for the card once more.

INSIDE THE VAULT

Your secrets, for as long as you need them.



INSIDE THE VAULT

This Card shows which card you opened, when it was last used and last written, and whether it has a Master Password.

"8 of 20 secrets" tells you how full the card is. **On card** means everything you see is saved on the card.

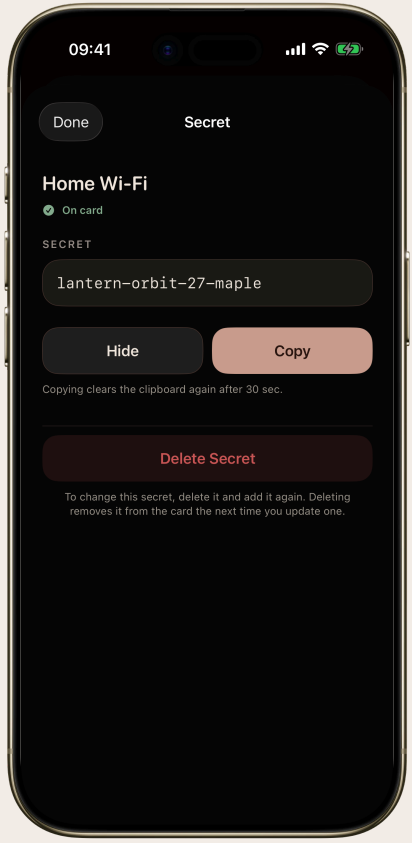
Search vault at the bottom finds a secret by name.

+ at the top adds a secret; ··· opens the **card menu**.

> **Decrypted only in memory.** Your secrets exist in readable form only while this window is open. Tap **Done** and they're gone from the phone.

READ AND COPY

Hidden until you ask.



READ AND COPY

Tap a secret to open it. The value is hidden behind dots.

Reveal shows it; **Hide** hides it again.

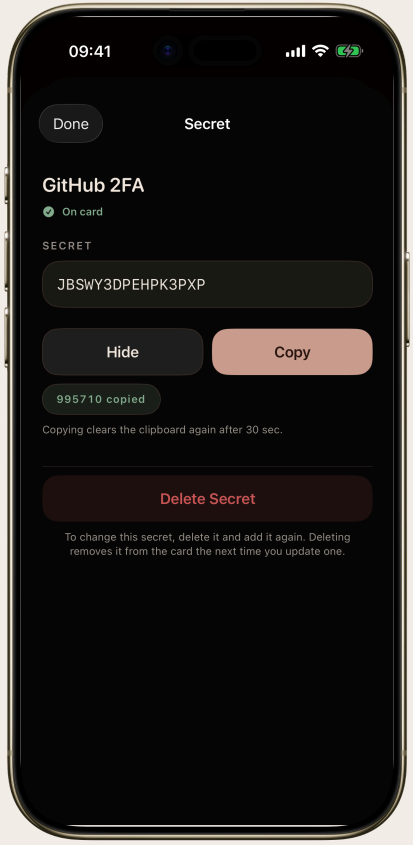
Copy puts it on the clipboard, and MI8OS **clears the clipboard again** after 30 seconds (change this in More: 15 sec, 30 sec or 1 min).

> **Paste quickly.** After the timer, the clipboard is empty, so the secret doesn't linger in other apps. The timer keeps running even if you close the vault before it ends.

> **Screen recording or mirroring?** MI8OS covers the screen and closes the vault, so secrets don't end up in a recording.

2FA CODES

Your authenticator, from the card.



2FA CODES

If a secret is a 2FA setup key, its page shows a **TOTP** button. Tap it and MI8OS calculates the current code and copies it, ready to paste.

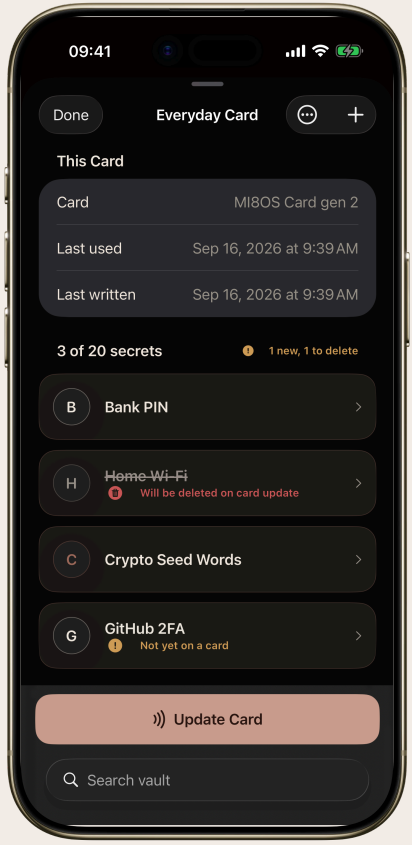
The card stores only the **encrypted setup key**. The code is calculated in the app after you've opened the vault, from the key and the current time, just like any authenticator app.

WHY THIS HELPS

If your authenticator codes are stored only on the phone you lose, they're gone with it. With the setup keys on your cards, you can get your codes on any new phone with the MI8OS app.

CHANGE THE VAULT

Add, delete, then Update Card.



CHANGE THE VAULT

Add: tap **+** and fill in name and secret.

Delete: swipe a secret left, or open it and tap **Delete Secret**. It stays in the list, marked, until you update the card. Changed your mind? Tap **Keep**.

Edit: there's no edit button on purpose. To change a secret, delete it and add it again.

Changes are marked as not yet written. Tap **Update Card** and hold the card to save them.

> **Closing with unwritten changes?** The app warns you: "Closing this card without updating it loses them."

KEEP EVERY COPY CURRENT

Each card is updated on its own.

Update Card writes to the card you opened, and only to that one. Your other cards still hold the previous version until you update them too.

GOOD HABIT

Once a year, open each card and check that all three show the same number of secrets.

KEEP EVERY COPY CURRENT

1 **CHANGE ONE CARD**

Open your Carry card, add or delete, tap **Update Card**.

2 **REPEAT FOR THE OTHERS**

Open your Home and Elsewhere cards and make the same change on each.

3 **SHORTCUT FOR NEW SECRETS**

Create a "new vault" with just the new secrets and save it to a card that already has your vault. Choose **Add Secrets**, and they're added to what's there.

04

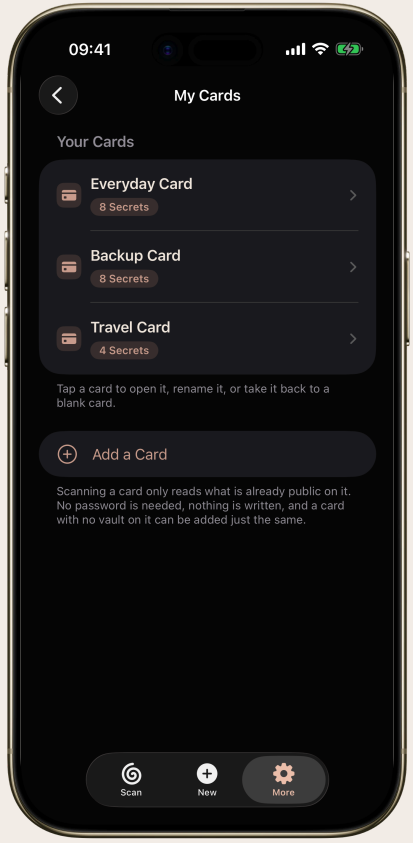
Manage your cards

Names, the card menu, reset, and the optional Master Password.

01 My Cards
02 The card menu ⋯
03 Reset a card
04 Lock a card · Master Password
05 Unlock a card · and a warning

MY CARDS

Give each card a name.



MY CARDS

In **More** → **My Cards** you see the cards this phone knows, with a tag: the number of secrets, **Empty**, or **Locked**.

Add a Card scans a card and remembers it. This only reads what is already public on the card: no password needed, nothing written.

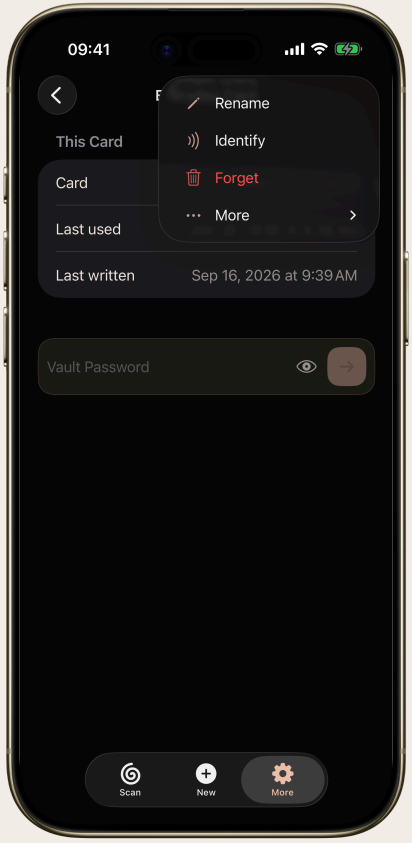
Tap a card to open it, rename it or reset it.

> **Faster opening.** A card this phone already knows opens with a single scan after you enter the password.

> **Stored on this phone only:** the names you gave, when cards were last used, and their public settings. Never a password, never a secret.

THE CARD MENU ···

Rename, identify, forget.



THE CARD MENU ···

RENAME

A name you'll recognise: "Carry", "Home", "Parents' safe".

IDENTIFY

Not sure which card is which? Tap Identify and hold a card. The app tells you if it's the one you're looking at, or which other card it is.

FORGET

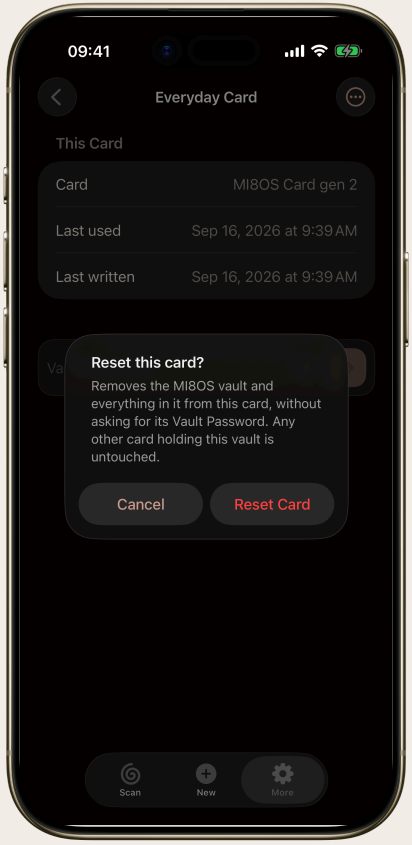
Removes the card from this phone's list. Nothing on the card changes, and you can add it again any time.

MORE

Reset Card, Lock Card and Unlock Card. See the next pages.

RESET A CARD

A clean card, ready for a new vault.



RESET A CARD

··· → **More** → **Reset Card** removes the MI8OS vault and everything else on the card, and frees all of its storage. It does **not** ask for the Vault Password.

Use it to:

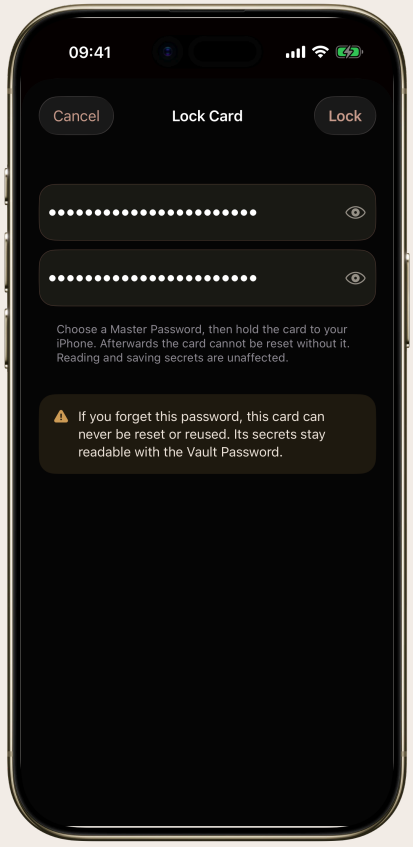
- ✓ Replace a vault completely with a new one
- ✓ Reuse a card after you forgot its Vault Password (the secrets on it are lost)
- ✓ Clear a card before giving it away

> **Other cards are untouched.** Resetting one card never affects the vault on your other cards.

> **Locked card?** It refuses to be reset until you enter its Master Password (next page).

LOCK A CARD · MASTER PASSWORD

Stop anyone from wiping your card.



LOCK A CARD · MASTER PASSWORD

Anyone who picks up an unlocked card can reset it, even without your Vault Password. They still can't read anything, but they could erase it.

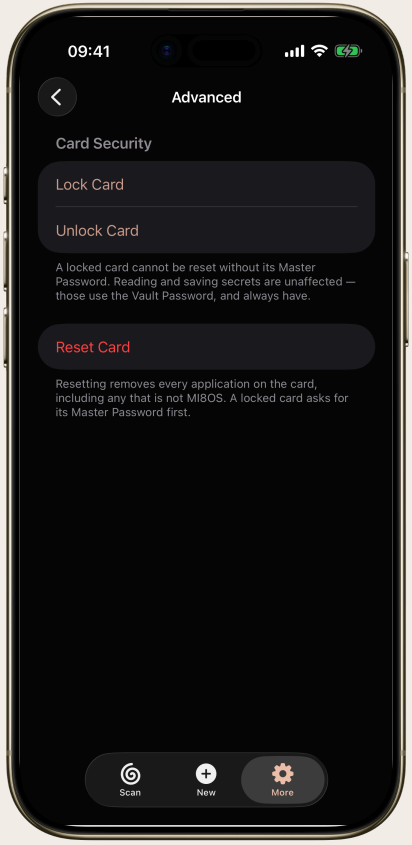
Lock Card prevents that. Choose a Master Password, hold the card, done. From then on, the card can't be reset or erased without it, by MI8OS or by anything else.

1. ··· → **More** → **Lock Card**
2. Enter a Master Password twice and tap **Lock**.
3. Hold the card until the app confirms "Card locked".

> **Reading and saving don't change.** Those still use the Vault Password only.

UNLOCK A CARD · AND A WARNING

Unlocking puts the card back to normal.



UNLOCK A CARD · AND A WARNING

··· → **More** → **Unlock Card**, enter the Master Password and hold the card. The card behaves like an unlocked one again. Its vault and Vault Password are unchanged.

To reset a locked card, choose Reset Card: the app asks for the Master Password, then formats the card.

DON'T FORGET IT

If you forget a card's Master Password, that card can **never** be reset or reused. Its secrets stay readable with the Vault Password. The app asks for it every time and never remembers it.

You can also lock, unlock and reset any card from **More** → **Advanced**, by scanning it.

05

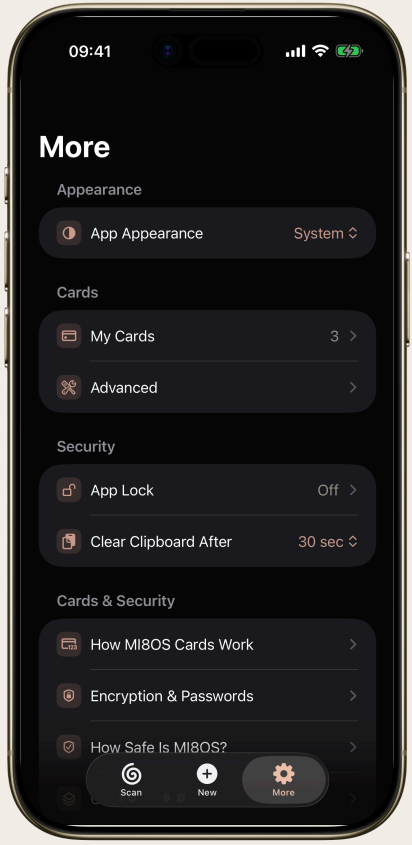
Settings

App Lock, Face ID, the clipboard, and how the app looks.

01 More
02 App Lock

MORE

Everything else, in one place.



MORE

App Appearance
System, Light or Dark.

My Cards
Your named cards.

Advanced
Lock, unlock or reset any card by scanning it.

App Lock
A PIN and Face ID for the app (next page).

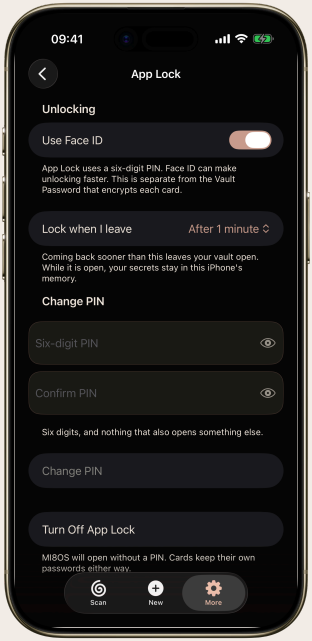
Clear Clipboard After
15 sec, 30 sec or 1 min after you copy a secret.

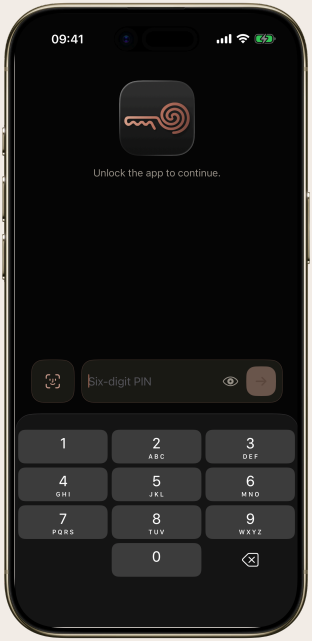
Cards & Security
Built-in help: How MI8OS Cards Work, Encryption & Passwords, How Safe Is MI8OS?, Card Care & Recovery.

Support & Legal
Order MI8OS Cards, Privacy Policy, Terms of Use.

APP LOCK

A lock for the app itself.





APP LOCK

Turn it on in More → App Lock: choose a six-digit PIN and, if you like, Face ID or Touch ID.

Lock when I leave: Immediately, after 1 minute or after 10 minutes. Leaving the app for longer closes any open vault, too.

The PIN only opens the app on this phone. It can't decrypt a card and doesn't replace a Vault Password. Pick six digits that don't also open something else.

06

How your secrets are protected

Two layers of encryption, one real example, and the honest answer to "what if someone steals my card?"

01 The big picture
02 From password to keys
03 Real example · 1 of 4 · The keys
04 If someone steals your card
05 Why your Vault Password matters
06 What MI8OS never does

THE BIG PICTURE

Two layers. Both come from your password.

1

IN THE APP: THE SECRETS ARE SEALED

Before anything is sent to the card, the app encrypts every secret on your phone with **ChaCha20-Poly1305** and a 256-bit key made from your Vault Password.

This is the main lock. Even someone holding the raw data sees only random-looking bytes, and any change to them is detected.

THE BIG PICTURE

2

ON THE CARD: THE DOOR IS LOCKED

The card's secure chip keeps the encrypted secrets behind its own **AES-128** key, also made from your Vault Password. It hands them out only after the phone proves it knows that key.

Without the right password, a reader gets nothing but the card's public settings.

Your Vault Password
never stored anywhere

↓

Content key
256-bit · seals the secrets (layer 1)

Card key
128-bit · opens the card's door (layer 2)

Management key
128-bit · manages the vault on the card

FROM PASSWORD TO KEYS

Why "Strengthening your encryption..." takes a moment.

Vault Password
+ a random 16-byte salt, different for every card

↓

Argon2id
64 MiB of memory · 3 passes · 4 lanes (RFC 9106)

↓

256-bit root key
exists only in memory, briefly

↓

HKDF-SHA256
splits the root into independent keys, each with its own label

↓

Content key
256-bit · for the secrets

Card key
128-bit · for the card's door

Management key
128-bit · for the vault's setup

FROM PASSWORD TO KEYS

ARGON2ID

A deliberately slow, memory-hungry password function. Every single guess costs 64 MiB of memory and real time, on your phone and on an attacker's computer alike.

THE SALT

Random bytes stored openly on the card. They make every card's keys unique, so nobody can prepare a table of guesses in advance.

REAL EXAMPLE · 1 OF 4 · THE KEYS

Let's encrypt "12345678".

These are real values, produced with the same algorithms and settings as the app. The password is for this example only.

VAULT PASSWORD

`copper-lantern-velvet-orbit`

SECRET NAME

`Demo PIN`

SECRET

`12345678`

SALT (RANDOM, ON THE CARD)

`7a8dbeec53e1eb50c70ccd4674a0e624`

REAL EXAMPLE · 1 OF 4 · THE KEYS

ROOT KEY (ARGON2ID)

84e743792af48790ce3ac4e2410ba1e9ef786851fa74467fc077208674905241

CONTENT KEY · 256-BIT

dcbe9b90a42a1c5e53f8bdaf07e3d763a61708ae3ad68fdfa7be72792fa6ab7c

CARD KEY · 128-BIT

266b550b4a87dd1029d53af4262244c1

MANAGEMENT KEY · 128-BIT

d9715ed54fbc71325587258c440a8dc6

> **None of these keys is ever stored.** The app calculates them when you enter your password and forgets them when the vault closes. Only the salt is on the card.

REAL EXAMPLE · 2 OF 4 · LAYER 1 IN THE APP

From "12345678" to random-looking bytes.

1. The secret is packed into 20 bytes: a name field and a secret field.

```
000  01 08 44 65 6d 6f 20 50 49 4e
010  02 08 31 32 33 34 35 36 37 38
```

field type and length · "Demo PIN" · "12345678"

REAL EXAMPLE · 2 OF 4 · LAYER 1 IN THE APP

2. ChaCha20-Poly1305 seals it with the content key, a unique 12-byte nonce (derived from the slot's header) and the header as authenticated data.

NONCE

`be00fc197a76fb68b8f315fa`

CIPHERTEXT · 20 BYTES

`5eda3e6b43d7aa61edf77ab4a26ae11e9b080c60`

TAG · 16 BYTES

`1b1b0dbbd23c5dffd6f4c462f9a449c4`

> **The tag is a seal.** If a single bit of the ciphertext or its header is changed, the tag no longer matches and the app refuses the data instead of showing something wrong.

REAL EXAMPLE · 3 OF 4 · WHAT'S ON THE CARD

One secret, one 192-byte slot.

This is exactly what the card stores for "Demo PIN". Look for "12345678": it isn't there.

```
000  31 0d ce db 3c 00 01 00 01 00 01 14
012  5e da 3e 6b 43 d7 aa 61 ed f7 7a b4
024  a2 6a e1 1e 9b 08 0c 60 1b 1b 0d bb
036  d2 3c 5d ff d6 f4 c4 62 f9 a4 49 c4
048  00 00 00 00 00 00 00 00 00 00 00 00
060  00 00 00 00 00 00 00 00 00 00 00 00
072  00 00 00 00 00 00 00 00 00 00 00 00
084  00 00 00 00 00 00 00 00 00 00 00 00
096  00 00 00 00 00 00 00 00 00 00 00 00
108  00 00 00 00 00 00 00 00 00 00 00 00
120  00 00 00 00 00 00 00 00 00 00 00 00
132  00 00 00 00 00 00 00 00 00 00 00 00
144  00 00 00 00 00 00 00 00 00 00 00 00
156  00 00 00 00 00 00 00 00 00 00 00 00
168  00 00 00 00 00 00 00 00 00 00 00 00
180  00 00 00 00 00 00 00 00 00 00 00 00
```

header: version, entry, position (12 bytes)

ciphertext (20 bytes) tag (16 bytes) empty space

REAL EXAMPLE · 3 OF 4 · WHAT'S ON THE CARD

BEHIND THE CARD'S DOOR

These slots live in the protected part of the card. The card only hands them out after the phone has passed its check with the card key (layer 2).

SAME SECRET, DIFFERENT BYTES

Write the same secret to another card, and it looks completely different, because each card has its own salt and keys.

REAL EXAMPLE · 4 OF 4 · THE PUBLIC PART

What anyone with a reader can see.

Each card also has a small public area (128 bytes). It's readable without a password, because the app needs the salt to make your keys.

```
000  4d 49 38 4f 53 03 32 b3 fb 93 6e bf
012  4d 64 b7 6f 5e 90 f5 75 7f 6e 00 00
024  01 00 c0 00 27 10 7a 8d be ec 53 e1
036  eb 50 c7 0c cd 46 74 a0 e6 24 00 01
048  00 00 00 00 00 03 04 00 20 00 00 00
060  00 00 00 00 00 00 00 00 00 00 00 00
072  00 00 00 00 00 00 00 00 00 00 00 00
084  00 00 00 00 00 00 00 00 00 00 00 00
096  00 00 00 00 00 00 00 00 00 00 00 00
108  00 00 00 00 00 00 00 00 00 00 00 00
120  00 00 00 00 00 00 00 00
```

"MI8OS" and format · vault ID · card layout · salt · Argon2id settings · unused

REAL EXAMPLE · 4 OF 4 · THE PUBLIC PART

AND WITH A WRONG PASSWORD?

Change just the last letter of the password and the card key becomes:

`883e65196d88bc9f1aae79acf8fa7c74`

instead of `266b550b4a87dd1029d53af4262244c1`. Nothing alike. The card refuses the check, sends no secrets, and nothing is written.

IF SOMEONE STEALS YOUR CARD

They have a card. Not your secrets.

There's no back door and no skeleton key. The only way in is to guess your Vault Password, and both layers make each guess expensive.

A

GUESSING THROUGH THE CARD

Every guess needs the physical card. The thief runs Argon2id for a guess, then asks the card. The card answers one attempt at a time over NFC. In our estimate that's about 20 attempts per second at most.

IF SOMEONE STEALS YOUR CARD

B TAKING THE CHIP APART

The expensive route. A specialised lab might try to extract the encrypted slots from the chip itself. Then they can guess offline, on many computers, but each guess still costs a full Argon2id run with 64 MiB of memory.

THE HONEST BOTTOM LINE

Both routes end at the same question: **how hard is your Vault Password to guess?** With a strong one, guessing it is practically out of reach. With a weak one, both layers only buy time. The next page shows how much.

WHY YOUR VAULT PASSWORD MATTERS

How long to try every possibility?

	THROUGH THE CARD ~20 guesses / s	LAB + HUGE COMPUTER RIG 1,000,000 guesses / s
Any password in a list of 1 billion leaked passwords, e.g. "Summer2026!!"	up to about 2 years; common ones much sooner	up to about 17 minutes; common ones within seconds
12 random digits	about 1,600 years	about 12 days
4 random words	millions of years	about 116 years

WHY YOUR VAULT PASSWORD MATTERS

THROUGH THE CARD	LAB + HUGE COMPUTER RIG
~20 guesses / s	1,000,000 guesses / s
12 random lowercase letters	
over 100 million years	about 3,000 years
5 random words	
longer than the universe has existed	about 900,000 years
6 random words	
longer than the universe has existed	about 7 billion years

Worst case for you: the time to try every possibility. "Random words" means picked by dice from a 7,776-word list. The guessing speeds are generous estimates for illustration. For scale: one guess took about 25 ms on a modern Apple M4 computer using 4 cores.

WHY YOUR VAULT PASSWORD MATTERS

RECOMMENDATION

Five or six random words. Never reuse it, never use song lyrics, names or dates.

AND WRITE IT DOWN

Keep a copy somewhere safe and separate from your cards. A forgotten Vault Password can't be recovered.

WHAT MI8OS NEVER DOES

Nothing to hack in the cloud. Because there's no cloud.

- ✓ **No account, no server.** The app makes no network connections at all.
- ✓ **No stored passwords.** Vault and Master Passwords are never saved, on the phone or the card.
- ✓ **No copy on the phone.** Decrypted secrets exist only in memory while a vault is open. One exception: a secret you copied stays on the clipboard until the timer clears it (15 sec to 1 min), even if the vault has closed.
- ✓ **No telemetry.** No tracking, no analytics.

WHAT MI8OS NEVER DOES

- ✓ **Locks when you leave.** Leaving the app closes the vault (immediately or after your chosen delay).
- ✓ **Covers its screen** in the app switcher, and while recording or mirroring.
- ✓ **Detects tampering.** Changed data fails the seal and is refused.
- ✓ **Uses only public, standard algorithms:** Argon2id, HKDF-SHA256, ChaCha20-Poly1305, AES-128.

THE OTHER SIDE OF NO BACK DOOR

If you lose every card, or forget the Vault Password, nobody can get your secrets back. Not you, not us. That's why you have three cards and a written-down password.

07

Care, Android and help

01 Card care and recovery
02 On Android
03 Troubleshooting

CARD CARE AND RECOVERY

Three cards, three places.

01 KEEP THEM APART

One card with you or close by, one at home, one somewhere else: with family, at work or in a safe. One fire or burglary can't take all three.

02 LOST A CARD?

The finder holds encrypted data. Make a replacement (see 03) to get back to three copies. If you worry someone knows the password, make new vaults with a new Vault Password the same way, then reset your old cards.

CARD CARE AND RECOVERY

03 MAKING A REPLACEMENT

The app can copy a vault to other cards only right after creating it. For a replacement later, create a new vault on a blank card and enter the same secrets again: open a working card to read them, and if you write anything down in between, destroy that note afterwards. Do it before you're down to your last copy.

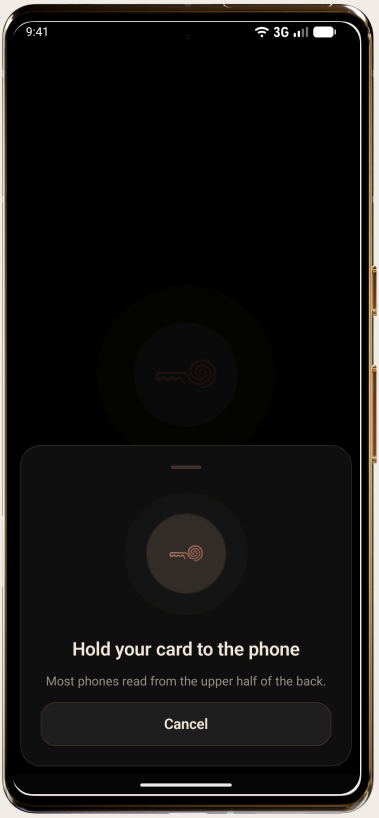
04 FORGOT THE VAULT PASSWORD?

Those secrets can't be recovered. If another card uses a password you still know, open that one. Otherwise reset the cards and start a new vault.

> **Look after the cards** like a bank card: no bending, no heat, no sharp edges. Keep them away from metal cases when you scan.

ON ANDROID

Same app, a few small differences.



ON ANDROID

The Android app is on **Google Play**. It works the same way and reads the same cards. A vault written on iPhone opens on Android, and the other way round.

Scanning

Android has no system NFC prompt, so MI8OS shows its own scan screen with a cancel button.

Card position

Hold the card to the upper half of the back of the phone. The exact spot varies by model.

NFC

NFC must be switched on in your phone's settings.

Biometrics

App Lock uses your phone's fingerprint or face unlock.

TROUBLESHOOTING

If something doesn't work.

The card isn’t detected

Hold it flat at the top edge of the iPhone and keep it still. Remove a thick or metal case. Try a little higher or lower.

The write stopped halfway

Tap **Try Again** and hold the same card still. Every save rewrites the whole card, and your changes stay in the app until it succeeds. If the app says the save can't be finished, **reset the card** and save again, or use a backup card and **replace this one**.

Wrong password

Check spelling and spaces. Remember: each card can have its own Vault Password.

TROUBLESHOOTING

"That is a different card"
You held another card than the one you opened. Use Identify to find the right one.

The card is full
A card holds 20 secrets. Delete one you no longer need, or split your secrets across cards.

A card won't reset
It's locked. Reset asks for its Master Password.

The vault closed by itself
You left the app, or the screen was being recorded. Open the card again.

The "Preparing your key" pause
Normal. It's the deliberate password strengthening.

More help · guide.mi8os.com

info@mi8os.com



MI8OS

Your privacy belongs with you.

MI8OS.COM

Inside MI8OS, mobile edition, English, October 2026. Describes the MI8OS app for iPhone and Android. Screens may differ slightly between versions. The example keys and bytes in chapter 06 were generated for this guide with a demo password; never use it. MI8OS · info@mi8os.com