



USER GUIDE

Loktra

Catch whoever tries to break into your phone — and keep the evidence in your own Google Drive. Here's everything you need to set it up and use it, in plain English.

Your phone. Your evidence. Your control.

Works on Android 7.0 and newer.

Updated August 2026 · App version 1.37

What's inside

01	What Loktra does	the idea in a nutshell
02	Getting started	install, set up, and switch it on
03	What happens during a break-in	how it catches someone
04	Your evidence	where it goes and how to view it
05	If your phone is lost or stolen	control it from anywhere
06	Free and Premium	what each plan includes
07	Make it yours	settings worth knowing
08	Keeping protection reliable	so it's always watching
09	Your privacy	our honest promise
10	Questions & troubleshooting	quick answers

01 What Loktra does

Most anti-theft apps just lock your phone. Loktra **catches the thief** — and makes sure the proof ends up somewhere only you can see it.

If someone picks up your phone and tries to get past your lock screen, Loktra takes a photo of them with the front camera — and, if you like, a short video and audio too. It tags where it happened and sends everything straight to **your own Google Drive**, then emails you a link. No one else ever sees it. Not even us.

THE ONE IDEA TO REMEMBER

Loktra protects **your own phone**, out in the open and honestly. It shows a small "protection active" notice by default and keeps a launcher entry. Premium owners can explicitly choose Stealth mode or a different launcher appearance after reading what each changes. It is **not** for spying on anyone else.

What makes it different

- **Evidence, not just a lock.** You get a face, a place, and a time — real proof.
- **It's yours alone.** Photos and video go only to your Google Drive, never to our servers.
- **You're in control.** Choose what it captures, how sensitive it is, and lock the app with a PIN or pattern.
- **It keeps watching.** It stays on after restarts and updates, even while your screen is off.

02 Getting started

Setup takes a couple of minutes. Loktra walks you through it in plain language the first time you open it.

- 1 Sign in with Google.** This is where your evidence will be delivered — your own Google Drive — and it lets you control the phone remotely later. Loktra never sends anything to us.
- 2 Allow it to catch break-ins.** Loktra asks to notice failed unlock attempts, and to use the camera and microphone so it can capture whoever's holding your phone.
- 3 Add the location (optional).** With this on, every capture is tagged with where your phone was.
- 4 Help it keep running.** Turn off battery optimisation and check the Permissions Centre. Android may require you to reopen Loktra after a restart before every background feature is available again.
- 5 Hold to arm.** On the Home screen, press and hold the big dial. It turns green — you're protected. A small notice appears to show it's active.

GOOD TO KNOW

You choose everything you grant, and you can change any of it later in your phone's Settings. Some protection features simply stop working without the permission they rely on — Loktra tells you which.

03 What happens during a break-in

Once armed, Loktra runs in the background with a visible "protection active" notice. Here's what happens the moment someone gets your unlock wrong.

- 1 Someone fails to unlock.** After the number of wrong attempts you've chosen (2 to 5), Loktra springs into action — without a shutter sound. Fingerprint, face and unknown biometric messages are counted separately, so different methods do not combine into one false threshold.
- 2 It captures the evidence.** A front-camera photo of the person, and — if you've turned them on — a short video with sound and an audio clip. You pick which of these it takes.
- 3 It notes the location.** Where your phone was when it happened, shown on a map.
- 4 It delivers to your Drive.** Everything is uploaded to your own Google Drive over a secure connection, and you get an email with a link.

WHICH UNLOCKS COUNT

Loktra reacts to a wrong **PIN, password, or pattern**. A pattern only counts if it connects at least four dots. Fingerprint and face unlock don't count as "wrong attempts" — that's how Android works — so set a PIN or pattern lock for the best protection. (You can also switch on an optional Premium feature that reads the lock screen's rejection message and reacts to repeated failed fingerprint/face attempts. Android never reports a failed fingerprint/face to apps, so Loktra does the best-effort, and success can vary by phone.)

04 Your evidence

Everything Loktra captures is yours — stored where only you can reach it.

Where it goes

Captures are uploaded to a folder called "**Loktra**" in your own Google Drive, and a link is emailed to you. They are **never** sent to Loktra's servers or seen by anyone else.

The Evidence tab

Open Loktra and tap **Evidence** to see every break-in, grouped by event, with the photo, video, audio, place and time. You can play a video right in the app, open the location on a map, or open the file in your Drive. Cloud-only media can stream without first keeping a permanent local copy. Mark important items as **Protected**, or delete what you don't.

After a reinstall or on another phone

Sign in to the same Google account and open Evidence. Loktra restores the gallery from your Drive, including event groups and Protected items. Devices on the same account share one Drive storage allowance, so the limit is consistent rather than multiplying for every phone.

A tidy footprint

Loktra caps how much space it uses on your phone (500 MB by default — you can change it). When it fills up, older unprotected evidence is cleared first to make room. Fresh evidence and Protected items are kept ahead of ordinary older items. Drive has its own limit, and deleting an item from Loktra can remove both its local and Drive copies.

05 If your phone is lost or stolen

From any other phone or computer, you can take charge of a lost device — as long as it's still switched on and online.

Open the **Loktra Command Center** at **loktra.app/remote** on any phone or computer and sign in with the same Google account. (Remote control lives only in this web portal — the app itself does not send commands to other devices.) You'll see your protected devices and can:

ACTION	WHAT IT DOES
Locate	Show the phone's current location on a map.
Ring	Sound a loud alarm, even if the phone is on silent.
Lock	Lock the screen immediately.
Capture	Take a fresh photo, video or audio right now (the phone must be armed).
Status	Check battery, connectivity, protection, storage and other security details.
Erase	Wipe the phone with Google Find My Device — see below.

ABOUT ERASING A LOST PHONE

For your security, modern Android only lets Google's own tool factory-reset a phone remotely. So when you need to erase a lost device for good, Loktra sends you straight to **Google Find My Device** (google.com/android/find), where you can wipe it in a couple of taps. Everything else — locate, ring, lock, capture — Loktra does itself.

SIM-change alerts

With Premium and phone-state access, removing a SIM or inserting a different one is treated as a theft signal. Loktra confirms that the change persists, captures evidence, uploads it and emails you. Removal and later insertion are separate opportunities to photograph whoever is handling the phone. Loktra compares device-local subscription and slot identifiers; it never reads your phone number, IMSI or ICCID.

Recovery after a reboot

Premium recovery can answer selected commands while the phone has rebooted but has not yet been unlocked: status, locate, start or stop the alarm, and lock. You can also queue a capture for the moment Android unlocks access to the camera and private app storage. Recovery must be armed in advance from the portal or app.

06 Free and Premium

Free protection catches an intruder. Premium adds richer evidence, remote recovery and advanced ways to keep a stolen phone reachable.

FREE INCLUDES	PREMIUM ADDS
Up to two front-camera photos per intrusion	Video, audio, rear camera and advanced capture settings
Evidence gallery, Google Drive delivery and optional Gmail alerts	Command Center: locate, ring, lock, capture and status
Default local intrusion alarm	SIM removal/swap alerts and pre-unlock recovery
App lock with PIN or pattern	Stealth mode, launcher disguise and lock-screen hardening
Newest 500 MB evidence view and 500 MB storage limits	Larger configurable device/Drive limits and Protected-history access

YOUR SETTINGS ARE NOT THROWN AWAY

If Premium ends, paid features stop or fall back safely, but most saved choices are kept so they can return if Premium resumes. The launcher is restored to Loktra rather than remaining disguised. Prices, trial eligibility and renewal terms are always shown by Google Play before purchase.

07 Make it yours

Loktra works great out of the box, but Settings let you tune it to how you use your phone.

SETTING	WHAT YOU CAN CHANGE
Failed attempts	How many wrong unlocks before it captures (2-5).
What to capture	Turn photo, video and audio on or off — pick any mix.
Photo & video	How many photos per capture, plus video length and quality.
Audio length	How long an audio clip runs.
Capture delay	A short pause first, to catch a clearer face.
Biometric timing	When experimental biometric detection is on, tune duplicate-message filtering from 500–1200 ms. The balanced default is 900 ms; experiment to find what works best on your phone.
On a break-in	Optionally sound an alarm or show a warning message to the intruder.
App lock	Use a PIN or pattern, with optional fingerprint quick unlock and device-credential recovery.
Email alerts	Choose whether Loktra sends evidence links through your own Gmail.
Storage limits	How much space Loktra may use on your phone and in Drive.
Appearance	Theme, language, and a Premium launcher disguise such as Calculator or Notebook.
Experimental	Optionally block the power menu/shade or catch failed biometrics; support varies by phone. Loktra has 21 app languages, but biometric detection must recognise the wording used by the phone's lock screen.

08 Keeping protection reliable

A thief can't be predicted, so Loktra is built to keep watching without you thinking about it — but a couple of phone settings help it stay rock-solid.

- **Check after a restart.** Android 15 and newer can block a camera service from starting automatically at boot. Loktra restores what the OS permits and tells you when opening the app is needed to return to full protection.
- **Allow it to run in the background.** Some phones (Xiaomi, Oppo, OnePlus, Samsung and others) aggressively close background apps to save battery. In Settings, allow Loktra to run in the background and turn off battery optimisation for it. Loktra's Reliability tips link you straight there.
- **Prevent unused-app hibernation.** Android can revoke permissions from apps it thinks are unused. The Permissions Centre shows the relevant system control.
- **Watch the status pills.** Home and Settings flag missing accessibility, background restrictions and other degraded states instead of silently claiming everything works.
- **Keep it charged-ish.** Like any app, Loktra can't protect a phone that's switched off or out of battery.

THE "PROTECTION ACTIVE" NOTICE

While armed, Loktra keeps a "protection active" notice in your notifications. This is intentional — it's how Loktra stays honest. If you turn on the optional **Stealth mode**, that notice goes away, so someone holding your locked phone sees no sign the phone is protected; Loktra explains exactly what that changes and asks you to confirm first. Either way the **app icon is always present** under either Loktra or the disguise you selected, and Android's own camera and microphone indicators still appear during every capture.

09 Your privacy

Loktra was built privacy-first. Here's the promise, in plain terms.

- **Your evidence stays yours.** Photos, video, audio and location go only to your own Google Drive (and an email link to you). They never touch our servers.
- **We store as little as possible.** To make sign-in and remote control work, we keep your account details and a list of your devices — nothing more, and never your media.
- **It protects one phone — this one.** Loktra can't be used to watch someone else's device.
- **It's owner-controlled.** Protection shows an active notice by default. You can opt into Stealth mode and can disguise the launcher icon and name; the launcher entry is never removed.
- **You can delete everything.** Sign out, remove the evidence from your Drive, or ask us to delete your account data any time.

FULL DETAILS

Read the full privacy policy at loktra.app/privacy, and request data deletion at loktra.app/data-deletion.

10 Questions & troubleshooting

Quick answers to the things people ask most.

I tried a wrong fingerprint and nothing happened.

That's expected — Android doesn't treat fingerprint or face as a "wrong attempt". Loktra reacts to a wrong PIN, password, or pattern (of at least four dots). You can also switch on the optional feature that reacts to repeated failed fingerprint/face attempts. Because it reads wording supplied by the phone maker, it is best-effort and may not work on every phone or language.

I forgot the PIN or pattern that locks Loktra.

Use **Forgot PIN/pattern?** and confirm with the phone's own secure screen lock. This clears Loktra's app lock without exposing the old secret. Fingerprint quick unlock is also optional when the phone has enrolled biometrics.

Loktra says it's not protecting after a while.

Your phone's battery saver may have closed it. Allow Loktra to run in the background and turn off battery optimisation for it — the Reliability section in Settings links you straight there.

Where are my captured photos?

In the "Loktra" folder in your Google Drive, and in the Evidence tab in the app. You also get an email with a link each time.

Can I erase my lost phone from here?

Yes — tap Erase in the Command Center and it takes you to Google Find My Device, which can factory-reset the phone remotely. Locate, ring, lock and capture all work from the Loktra web portal.

Does Loktra work if the phone is offline?

Catching a break-in and saving the evidence works offline — it uploads to your Drive as soon as the phone is back online. Remote control (locate, lock, ring) needs the phone to be online.

I reinstalled Loktra. Is my evidence gone?

No. Evidence already delivered to your Drive stays there. Sign in with the same Google account and open Evidence to restore the cloud gallery. Files that never uploaded before the uninstall cannot be recovered.

Why did SIM removal and reinsertion both create an alert?

That is intentional. Removing a SIM and inserting one are two separate moments when the person handling a stolen phone may be visible, so each persistent event can capture evidence.

Is this legal / allowed on Google Play?

Yes. Loktra protects only your own phone, shows a visible notice and icon, and never spies on anyone else — fully in line with Google Play's policies.

NEED A HAND?

Visit **loktra.app** for the latest help, the privacy policy, and how to reach us.