SETUP GUIDE

Mobile Device Security Setup Guide for Web3 Teams

Securing the phone: authenticators, passkeys, wallets, and sessions

Prepared for	Web3 team members	Classification	Internal
Prepared by	Oak Security	Date	2026-06-17

Oak Security GmbH

1. What This Guide Is For

This guide is for anyone in a Web3 team who uses a phone for work, whether you are a developer, an operator, or in a non-technical role. The phone is not a secondary device. It holds your authenticator codes, your passkeys, your wallet apps, and your live work sessions for email, chat, source control, and cloud consoles. For most teams it is also the second factor that protects everything else.

That makes the phone a high-value target. Attackers go after it directly through SIM-swap and number-transfer fraud, through malicious or over-permissioned apps, and through phishing links delivered by SMS and chat. A compromised phone can hand over your 2FA, your synced passkeys, and an unlocked path into accounts the laptop baseline was meant to protect.

> **NOTE**
>
> **Baseline rule:** any phone used for work should be encrypted, locked with biometrics plus a strong passcode, kept to a minimal set of vetted apps, hardened against SIM-swap, and separated from personal activity.

For the most sensitive work, such as treasury signing, production administration, and cloud or KMS access, the phone should not be the device that signs or approves anything. Section 8 covers the stricter profile for those users.

2. iOS vs Android Baseline

Modern iOS and Android devices encrypt storage by default and offer strong biometrics, automatic updates, and remote wipe. The platforms differ in where settings live, how tightly app sources are controlled, and how management works. The security goals are identical; the menus and the failure modes are not.

Topic	iOS	Android
Encryption	On by default on modern devices; tied to the passcode.	On by default (file-based encryption) on modern devices; tied to the screen lock.
App sources	Single official store by default. Sideloading and alternative marketplaces exist in some regions but are the exception.	Official store by default, but sideloading of APKs and third-party stores is built in and widely used. Larger attack surface.
Enterprise app abuse	TestFlight and enterprise (developer) certificate distribution can push apps outside the store.	Sideloaded APKs and unknown-source installs are the main vector.
Account behind the device	Apple Account.	Google Account.
Find and wipe	Find My.	Find My Device.
Work separation	Managed Apple Account or MDM separation of work apps and data.	Work profile (Android Enterprise) isolates work apps, data, and accounts in a separate container.

Managed vs Personal Devices

A managed device is enrolled in company MDM or carries a company work profile. The organization can enforce encryption, lock policy, app allowlists, and remote wipe, and can cleanly remove work data at offboarding. A personal device used for work (BYOD) puts the same controls on the user.

This guide assumes most phones are personal. Apply the baseline yourself. For critical-access users, a managed or dedicated device is the better option, and Section 8 says so.

3. Quick Setup Checklist

These are the settings every work phone should have before it is used for work.

Lock, Biometrics, and Encryption

Setting	iOS	Android
Passcode / PIN	Set a 6-digit or longer numeric passcode, or an alphanumeric one. Avoid 4-digit. **Settings > Face ID & Passcode**.	Set a 6-digit PIN or longer, or a strong password. Avoid pattern unlock. **Settings > Security**.
Biometrics	Enable Face ID or Touch ID. Biometrics unlock; the passcode is the real secret. **Settings > Face ID & Passcode**.	Enable fingerprint or face unlock as convenience; keep a strong PIN or password as the fallback. **Settings > Security**.
Auto-lock	Set the shortest auto-lock you can tolerate. **Settings > Display & Brightness > Auto-Lock**.	Set a short screen timeout and lock-after-timeout. **Settings > Display** and **Settings > Security**.
Encryption	On by default; confirm a passcode is set, which is what enables it.	On by default on modern devices; confirm a screen lock is set, which is what protects the keys.

Updates and App Sources

Setting	iOS	Android
OS updates	Install pending updates. Turn on automatic updates. **Settings > General > Software Update**.	Install pending system and Google Play system updates. Turn on automatic updates. **Settings > System > Software update** and Play system update under **Security**.
App updates	Enable automatic app updates.	Enable automatic app updates in the Play Store.
App sources	Install only from the official	Keep "install unknown apps"

	store. Do not install enterprise-certificate or TestFlight apps for work unless the team approves them.	disabled for every app. Use only the official store. Avoid third-party APK sources. **Settings > Apps > Special app access > Install unknown apps**.

SIM, Find-My, and Remote Wipe

Setting	iOS	Android
SIM lock	Set a SIM PIN so a removed physical SIM cannot be reused. **Settings > Cellular > SIM PIN**.	Set a SIM PIN. **Settings > Security > SIM card lock**. (For eSIM, see Section 5.)
Carrier port-out lock	Set a carrier account PIN and port-out / number-transfer lock with your carrier. See Section 5.	Same: set carrier PIN and number-transfer lock. See Section 5.
Find / remote wipe	Enable Find My, including the network and Send Last Location. **Settings > [your name] > Find My**.	Enable Find My Device. **Settings > Security > Find My Device**.

4. Authenticators, Passkeys, and Wallet Apps

The phone is where 2FA codes, passkeys, and hot wallets live. Treat each by its real risk level, not by how convenient it feels.

Where Your Second Factors Live

Factor	What It Is	Caveat
TOTP authenticator codes	App-generated 6-digit codes (the standard authenticator apps).	If the authenticator backs up to the cloud, the codes are only as strong as that cloud account and its 2FA. A device-bound authenticator is stronger but harder to recover.
Synced passkeys	Passkeys stored in the platform keychain or a password manager and synced across devices.	A synced passkey is a credential that follows your platform account. For critical accounts, prefer a hardware security key.
Device-bound passkeys / hardware keys	Passkeys bound to this device's secure element, or an external hardware security key.	Strongest, because the private key cannot be exported. Less convenient; needs backup keys.
SMS codes	One-time codes by text message.	Weakest. Vulnerable to SIM-swap and interception. Move critical accounts off SMS (Section 5).

Decide consciously whether your authenticator backs up to the cloud. Cloud backup helps you survive a lost phone but ties all your codes to one account; that account then needs its own hardware-backed 2FA. Device-bound is stronger against remote compromise but requires a tested recovery plan.

Wallet Apps

- A mobile wallet app should hold a hot balance only: an amount you can afford to lose if the phone is compromised. Meaningful value belongs behind a hardware wallet.
- Do not store or photograph a seed phrase on the phone. No Notes, no screenshots, no cloud-synced album, no chat.
- Keep wallet apps to the ones you actually use. Each extra wallet is extra attack surface and another approval prompt you might rubber-stamp.

WalletConnect Hygiene

- Only scan a WalletConnect QR code or follow a connection link you initiated, from a site you reached yourself. Treat unsolicited QR codes and connection prompts as phishing.
- Read what you are approving. Connection scope, the requested network, and each signature request are your last checkpoint before a malicious dapp drains a hot wallet.
- Review and disconnect stale sessions in the wallet's connections list. An old live session is a standing grant.

App Provenance

- Install wallet and authenticator apps only from the official store, and verify the publisher. Fake wallet and authenticator clones are a recurring app-store and search-ad problem.
- **Android sideloading** is the single largest mobile-malware vector. Keep "install unknown apps" off. A sideloaded "wallet" or "airdrop" APK is the classic delivery method for seed-stealers and clippers.
- **iOS enterprise-certificate and TestFlight abuse** is the iOS equivalent. An enterprise (developer) certificate or a configuration profile (MDM profile) can install an app that never passed store review and can carry broad device privileges. Do not install one because a chat told you to. Review installed profiles under **Settings > General > VPN & Device Management** and remove anything you do not recognize.

5. SIM-Swap and Account-Takeover Defense

SIM-swap (also called number transfer or port-out fraud) is when an attacker convinces your carrier to move your phone number to their SIM or eSIM. Once they hold your number, any SMS 2FA and any phone-number recovery flow is theirs. This is one of the most common paths to a Web3 account takeover.

Carrier Hardening

- Set a carrier account PIN or passcode that is required for any account change.
- Enable the carrier's port-out / number-transfer lock or "number transfer PIN." Names differ by carrier; the FTC's guidance covers what to ask for.
- Do not reuse the SIM PIN or your device passcode as the carrier PIN.

Move Off SMS

- Move every critical account off SMS 2FA to a TOTP authenticator, a passkey, or a hardware security key. Critical accounts include email, password manager, source control, cloud, registrar, exchange, and any treasury tooling.
- Where a service forces a phone number on file, remove SMS as a usable second factor and as a recovery method if the service allows it.

Do Not Anchor Recovery to the Number

- Do not use your phone number as a recovery factor for critical accounts. A number you can lose to a carrier rep is not a root of trust.
- Use recovery codes stored in the password manager, and platform recovery contacts where supported, instead of SMS recovery.

eSIM Considerations

- An eSIM removes the physical-SIM theft path but does not remove SIM-swap. An attacker who social-engineers the carrier can provision your number onto their own eSIM. Carrier port-out lock still matters.
- Protect the carrier account and the email tied to it as critical accounts in their own right.

Harden the Account Behind the Device

The Apple Account or Google Account behind the phone can unlock everything on it.

Control	iOS (Apple Account)	Android (Google Account)
Strong unique password	Yes, in the password manager.	Yes, in the password manager.
Hardware-backed 2FA	Use the strongest 2FA available; prefer a security key for highly targeted users.	Enroll a security key; consider Advanced Protection for highly targeted users.
Recovery review	Review recovery contacts, recovery key, trusted phone numbers, and trusted devices.	Review recovery email and phone, and remove stale entries.
Device list	Remove old or unused devices from the account.	Remove old or unused devices from the account.

6. App and Permission Hygiene

Most mobile compromise after the lock screen comes through apps you installed and permissions you granted. Review both.

Permissions To Watch

Permission	Why It Matters
Accessibility services (Android)	The most abused permission on Android. It lets an app read screen content and act as the user: read 2FA codes, click through approvals, capture what you type. Grant it only to apps that genuinely need it, and never to one you were told to install over chat.
Screen recording / screen capture	An app that can record the screen can capture seed phrases, codes, and private chats.
Clipboard access	Wallet addresses and one-time codes pass through the clipboard. Clipboard-watching malware swaps a copied address for the attacker's (″clipper″ malware). Some platforms warn on clipboard reads; pay attention.
Notifications	Notification access can expose 2FA codes and message previews on the lock screen. Hide sensitive previews.
Default keyboard	A third-party keyboard can log everything you type, including passwords and seed words. Use the system keyboard for sensitive entry.

Provenance and Over-Permissioning

- Prefer the system keyboard and the system clipboard manager. Third-party keyboards and clipboard managers are a known data-exfiltration channel.
- Question apps that ask for more than their function needs: a flashlight that wants accessibility, a ″wallet helper″ that wants screen recording, a QR scanner that wants your contacts.

- Periodically review the permission dashboard (**Settings > Privacy & Security** on iOS, **Settings > Privacy > Permission manager** on Android) and revoke what is not needed.
- Remove apps you no longer use. Uninstalled is the only permission you never have to audit.

7. The Recommended Setup Flow

Step 1: Update the OS

Install pending OS and app updates, then turn on automatic updates. On iOS: **Settings > General > Software Update**. On Android: **Settings > System > Software update**, plus the Google Play system update under **Security**.

Do not sit on security updates. Mobile exploit chains are patched in these releases; an unpatched phone is the easy target.

Step 2: Set Lock, Biometrics, and Verify Encryption

Set a strong passcode or PIN (6 digits or longer, or alphanumeric; avoid 4-digit and avoid pattern unlock). Enable Face ID, Touch ID, or fingerprint as the convenience layer. Set the shortest auto-lock you can tolerate.

Storage encryption is on by default on modern devices and is tied to that lock. Setting a real passcode is what makes the encryption meaningful.

Step 3: Set SIM Lock and Migrate 2FA Off SMS

Set a SIM PIN. Call or message your carrier and set a carrier account PIN plus a port-out / number-transfer lock.

Then move every critical account off SMS 2FA to a TOTP authenticator, a passkey, or a hardware security key, and stop using your phone number as a recovery factor for those accounts. This is the highest-value step in this guide.

Step 4: Clean Up Apps and Review Permissions

Uninstall apps you do not use. For the rest, review permissions, with priority on accessibility services (Android), screen recording, clipboard, notifications, and default keyboard. Revoke anything an app does not need.

On Android, confirm "install unknown apps" is off for every app. On iOS, open **Settings > General > VPN & Device Management** and remove any profile or enterprise app you do not recognize.

Step 5: Set Up Authenticators and Wallets Correctly

Install authenticator and wallet apps only from the official store, and verify the publisher. Decide whether your authenticator backs up to the cloud, and if it does, protect that account with hardware-backed 2FA.

Keep mobile wallets to a hot balance only. Do not store or photograph a seed phrase on the phone. Review WalletConnect sessions and disconnect stale ones.

Step 6: Enable Find-My and Remote Wipe

Turn on Find My (iOS) or Find My Device (Android), including location and the option to wipe remotely. Confirm you can reach the web console and that you know your account password, so you can locate, lock, or wipe a lost device from somewhere else.

Step 7: Separate Work and Personal

Keep work and personal apart on the phone.

- On Android, use a work profile (Android Enterprise) for work apps and accounts. It isolates work data in a separate container that the team can wipe without touching personal data.
- On iOS, use managed Apple Accounts or MDM separation where the team provides it; otherwise keep work accounts and personal accounts distinct, and do not log personal wallets into the same context as work sessions.
- Do not mix personal wallet activity and random dapps with the phone that holds your work 2FA and live work sessions.

8. Extra Rules for Critical-Access Users

Some people hold access where a phone compromise becomes a company-level incident: treasury signers, production administrators, release owners, DNS or registrar admins, source-control organization admins, and anyone with cloud, KMS, or signing authority.

If this applies to you, the phone is not a signing device.

Control	Requirement
No treasury signing from the phone	Do not sign treasury or multisig transactions from a mobile wallet. Sign via a hardware wallet, with verification on the hardware screen.
Dedicated device	Use a dedicated phone for privileged work where practical, kept minimal and separate from personal use.
No SMS 2FA anywhere	No critical account uses SMS as a second factor or as a recovery method.
Hardware-backed MFA	Use hardware security keys or device-bound passkeys for critical accounts. Do not treat synced passkeys as equivalent.
Minimal app surface	Install only the apps the role requires. No sideloaded apps, no enterprise-certificate apps, no third-party keyboards.
Carrier hardening	Carrier PIN and port-out / number-transfer lock set and verified.
Account behind the device	Apple or Google Account on the strongest available protection, with recovery and device lists reviewed.
Lockdown Mode	Consider iOS Lockdown Mode if you are highly targeted and can tolerate the usability impact.
Travel	Do not travel with the signing device, the recovery material, and the primary phone together.

Suspicious activity	Rotate relevant credentials and revoke sessions before resuming privileged work.

9. Things To Avoid

These habits are common, and each one is a known mobile attack path.

- Using SMS 2FA for critical accounts, or leaving a phone number as a recovery factor.
- Keeping meaningful value in a mobile wallet instead of behind a hardware wallet.
- Storing or photographing a seed phrase on the phone.
- Sideloading apps on Android, or enabling "install unknown apps."
- Installing enterprise-certificate apps, configuration profiles (MDM profiles), or TestFlight builds on iOS because a chat or website told you to.
- Scanning random WalletConnect QR codes or accepting connection prompts you did not initiate.
- Granting accessibility services, screen recording, or clipboard access to apps that have no reason to need them.
- Installing third-party keyboards or clipboard managers and using them for sensitive entry.
- Charging at public USB ports without a data-blocker or charge-only setting (juice-jacking).
- Tapping links in SMS, DMs, or unexpected messages, including "delivery," "security alert," and "airdrop" lures.
- Approving wallet signature requests without reading what they actually authorize.

10. If Something Suspicious Happens

For a lost or stolen phone, or a suspected compromise, move fast and use a different trusted device for the recovery steps. Assume the phone's 2FA and sessions are in the attacker's hands until proven otherwise.

Immediate

1. From another trusted device, sign out of and revoke sessions for the accounts used on the phone.
2. Use Find My or Find My Device to locate, lock, and if needed remotely wipe the phone.
3. If you cannot wipe it quickly, change the password and revoke sessions for the Apple or Google Account behind the device first; that account is the master key.

Contain

- Execute the SIM-swap response: call the carrier, confirm the number has not been ported, and lock the carrier account. If the number was ported, treat every SMS-based factor and recovery flow as compromised.
- Move any hot-wallet funds on the phone to a safe address from a clean device.
- Disconnect active WalletConnect sessions.
- Notify the security owner or head of engineering from a clean device.

Rotate

Rotate anything that may have been exposed:

Item	Action
Apple / Google Account	Rotate the password, review 2FA, recovery contacts, and the device list.
Email / workspace	Sign out all sessions, rotate the password, review OAuth apps and forwarding rules.
Authenticator-protected accounts	Re-enroll 2FA on new factors if the authenticator was on the phone.

Source control / cloud / registrar	Revoke sessions and tokens, rotate credentials, review recent activity.
Passkeys	Remove device-bound passkeys registered from the phone; re-register from a clean device.
Wallets	Treat hot wallets on the phone as compromised. Move funds and stop using those keys.

If compromise cannot be ruled out, wipe and set up the phone from scratch, reapply this baseline, and reconnect accounts only after old sessions have been revoked. Critical-access users should not resume privileged work until the security owner agrees it is safe.

11. Monthly Self-Check

Once a month, do this short review. It should take a few minutes.

Check	Done
The OS and apps are up to date.	
A strong passcode or PIN is set, with biometrics enabled.	
Auto-lock is set to a short timeout.	
A SIM PIN and a carrier port-out / number-transfer lock are set.	
No critical account uses SMS 2FA or a phone-number recovery factor.	
Critical accounts use a TOTP authenticator, passkey, or hardware key.	
Authenticator cloud-backup status is understood and the backing account is protected.	
Mobile wallets hold only a hot balance; no seed phrase is on the phone.	
WalletConnect sessions have been reviewed and stale ones disconnected.	
App permissions (accessibility, screen recording, clipboard, keyboard) have been reviewed.	
No sideloaded, enterprise-certificate, or unrecognized profile apps are installed.	
Find My / Find My Device and remote wipe are enabled.	
The Apple / Google Account behind the device is hardened and its device list reviewed.	
Work and personal activity are separated on the device.	

12. References

- Apple Platform Security: https://support.apple.com/guide/security/welcome/web
- Apple iOS and iPadOS security overview: https://support.apple.com/guide/security/intro-to-apple-platform-security-seccd5016d31/web
- Android security overview: https://source.android.com/docs/security/overview/
- Android file-based encryption: https://source.android.com/docs/security/features/encryption/file-based
- Google Account security and 2-Step Verification: https://support.google.com/accounts/answer/185839
- Google Advanced Protection Program: https://landing.google.com/advancedprotection/
- Android Enterprise work profile: https://support.google.com/work/android/answer/6191949
- Apple Lockdown Mode: https://support.apple.com/en-us/105120
- FTC SIM swap guidance: https://consumer.ftc.gov/articles/sim-swap-scams-how-protect-yourself
- FTC cell phone fraud and number-transfer protection: https://consumer.ftc.gov/articles/cell-phone-fraud
- WalletConnect (Reown) security: https://walletconnect.com/security
- WalletConnect (Reown) documentation: https://docs.walletconnect.network/