

Smartphone Security Playbook

Lock Down, Recover, and Protect the Device That Controls Half Your Digital Life

Your phone is not just a phone.

It's an account-recovery device, authenticator, wallet, camera, password vault, location tracker, and remote control for a large part of your digital life. This playbook turns the Smartphone Security Quick-Start Checklist into a practical lockdown and recovery plan.

For iPhone and Android

The Grumpy Sysadmin

Version: August 2026

Menu names can vary by iOS/Android version, phone manufacturer, carrier, and region. Use Settings search if a label has moved.

How to Use This Playbook

The quick-start checklist tells you what deserves attention. This playbook explains what the settings mean, what to change, how to verify the change, and how to recover when the phone is lost, stolen, damaged, traded in, or replaced.

Don't try to make twenty security changes in five minutes and then discover that you've locked yourself out of your own accounts. Work through the sections in order, verify each change, and record the recovery information outside the phone.

Grumpy Rule: Security that only works while you still have the phone isn't a recovery plan.

The Order Matters

- Secure the screen lock first.
- Secure the Apple Account or Google Account next.
- Make sure you can recover that account without relying only on this phone.
- Turn on finding, locking, and erasing features.
- Verify backups and authenticator recovery.
- Review apps, permissions, updates, and carrier protection.
- Write down the emergency sequence before you need it.

What You Need Before You Start

Preparation	Done
The phone is charged and connected to a trusted network	☐
You know the phone passcode/PIN	☐
You know the Apple Account or Google Account password	☐
You can access the account recovery email or trusted phone number	☐
You have a second trusted device or computer available for verification	☐
You have somewhere outside the phone to store recovery codes and emergency instructions	☐

Table of Contents

- 1. Lock the Phone Properly
- 2. Secure the Apple or Google Account
- 3. Turn On Find, Lock, and Erase Features
- 4. Protect Backups, Photos, Contacts, and Authenticator Access
- 5. Review Apps and Permissions
- 6. Install Updates and Check Device Support
- 7. Lock Down the Phone Carrier Account
- 8. Reduce Scam, Public Wi-Fi, and Charging Risk
- 9. Prepare for Loss, Theft, Damage, or Replacement
- 10. Family Smartphone Security
- 11. Emergency Response Worksheets
- 12. Final Verification and Maintenance

1. Lock the Phone Properly

Start with the screen lock. If someone can open the phone, many of the protections inside it become considerably less impressive.

Grumpy Rule: A phone protected by 1234 isn't locked. It's politely asking the thief to count.

Choose a Strong Screen Lock

Use a passcode, PIN, or password that can't be guessed from your birthday, address, phone number, or a repeating pattern. Biometrics are convenient, but the underlying passcode still matters because it can be used when biometrics are unavailable.

iPhone

1. Open Settings and choose Face ID & Passcode or Touch ID & Passcode.
2. Confirm that a device passcode is enabled. If you are using a weak or reused code, choose Change Passcode.
3. Use Face ID or Touch ID for normal unlocking if you're comfortable doing so.
4. Review the items allowed while the phone is locked. Disable lock-screen access to features you don't want available without authentication.
5. If your iPhone supports Stolen Device Protection, review and enable it. Consider the option that requires additional protections even away from familiar locations.

Android

1. Open Settings and search for Screen lock, Device unlock, or Lock screen.
2. Choose a PIN, password, or supported secure lock method. Avoid simple patterns and predictable PINs.
3. Set up fingerprint or face unlock if your phone supports a strong implementation and you want the convenience.
4. Set the phone to lock quickly after the screen turns off.
5. Search Settings for Theft protection or theft-prevention features and review what your device supports.

Hide Sensitive Lock-Screen Notifications

A locked phone can still leak one-time codes, message previews, medical information, financial alerts, and names of contacts. You don't need to make the lock screen useless; you need to keep sensitive content from becoming free reading material.

iPhone

1. Open Settings > Notifications > Show Previews.
2. Choose When Unlocked or another privacy level appropriate for you.
3. Review individual apps that should never show sensitive content on the lock screen.

Android

1. Open Settings and search for Lock screen notifications or Notifications on lock screen.
2. Choose to hide sensitive content or show notifications only after unlock, depending on your device.
3. Review banking, email, authenticator, password-manager, health, and messaging apps individually.

Quick verification

Lock the phone. Have someone else look at the screen. Can they read a verification code, email preview, private message, or financial alert without unlocking it? If yes, keep adjusting.

2. Secure the Apple or Google Account

The main account connected to the phone controls backups, app purchases, device tracking, account recovery, and often several other devices. Protect it before someone else decides to become the account owner.

Grumpy Rule: *If the only way to recover the account is a code sent to the phone you just lost, that's not recovery. That's a scavenger hunt with no prize.*

Use a Unique Password and MFA

The Apple Account or Google Account password should be strong and unique. Do not reuse the same password for email, shopping, social media, or anything else. Multi-factor authentication should be enabled, but recovery must not depend on one device.

Apple Account

1. Open Settings and tap your name.
2. Open Sign-In & Security.
3. Review the Apple Account password and change it if it's reused or weak.
4. Review Two-Factor Authentication, trusted phone numbers, and trusted devices.
5. Add a second trusted phone number when practical so losing one phone doesn't become an account-recovery disaster.

Google Account

1. Open Settings > Google or open your Google Account from a browser.
2. Open Security.
3. Review the password, 2-Step Verification methods, recovery phone, and recovery email.
4. Create backup methods that don't depend solely on the phone you are protecting.
5. Review devices signed into the account and sign out devices you no longer own or recognize.

Review Trusted Devices and Recovery

Account Recovery Review	Done
Recovery email is current and accessible	☐
Recovery phone number is current	☐
At least one recovery method works without this phone	☐
Old devices and sessions were removed	☐
Backup codes or equivalent recovery information are stored safely	☐
A password manager can be accessed from another trusted device	☐
A trusted family member knows where emergency recovery instructions are stored	☐

3. Turn On Find, Lock, and Erase Features

A lost phone is much easier to handle when location and remote-protection features were enabled before it vanished.

Grumpy Rule: Device tracking configured after the phone disappears is wonderfully useless. Prepare before the phone begins its independent travel career.

iPhone - Find My

1. Open Settings, tap your name, and open Find My.
2. Open Find My iPhone and confirm the finding features are enabled as appropriate for your device.
3. From another trusted device or browser, verify that the iPhone appears in Find My.
4. Learn where Mark As Lost/Lost Mode is located before you need it.
5. Understand that remote erase is a last-resort action when recovery is unlikely and the data risk is more important than getting the device back.

Android - Find Hub / device finding

1. Open Settings and search for Find Hub, Find My Device, or device finding.
2. Confirm the feature is enabled and that the phone is associated with the correct Google Account.
3. From another trusted device or browser, verify that the phone appears in Google's device-finding service.
4. Learn how to mark the device lost/secure it and how to erase it remotely if recovery fails.
5. Review theft-protection options supported by your phone, because available features vary by Android version and manufacturer.

Record the Device Identity

Record the phone model, serial number, and IMEI somewhere that's not the phone. This information can help with carrier, insurance, police-report, and replacement workflows.

Device Record	Done
Manufacturer and model	☐
Phone number	☐
Serial number	☐
IMEI	☐
Carrier	☐
Apple Account or Google Account used on the device	☐
Insurance/warranty provider and policy information, if applicable	☐