Stolen phone checklist

What to do if your phone is stolen. Work down the list in order and tick each step as you finish it. The full guide, with the reasons behind every step, is at confirmedstolen.com/stolen-phone/.

In the first hour

- [ ] **Mark the phone as lost from another device or a browser**
  For an iPhone, sign in at iCloud.com/find (www.icloud.com/find) and choose Mark as Lost. For Android, use the Find Hub app on another device or android.com/find (www.android.com/find) and choose Mark as lost.

- [ ] **Leave contact details off the lock screen if the phone was stolen**
  Apple warns that a thief could use a phone number or message on the lock screen for social engineering. Add contact details only if you believe the phone was simply lost.

- [ ] **Do not remove the phone from Find My or Find Hub**
  On an iPhone, removing the device also removes Activation Lock, which makes the phone easier to erase and resell.

- [ ] **Do not go to the location shown on the map**
  Apple advises against trying to recover a stolen device yourself. Give the location to local law enforcement instead.

- [ ] **Call your carrier from another phone to suspend service**
  Use the number on your bill or the carrier's official website. Ask it to suspend the line so the SIM cannot be used for calls, texts or verification codes.

- [ ] **Ask the carrier to block the IMEI and lock your number**
  Ask it to report the IMEI to the device block list, and to add an account PIN and port-out lock so no one can move your number. See our SIM swap guide (confirmedstolen.com/sim-swap/).

- [ ] **Change your primary email password from a trusted device**
  Email is the master key for other password resets. Sign out of all sessions and remove recovery phone numbers or forwarding rules you did not set.

Within 24 hours

- [ ] **Call your bank and card issuers on their official numbers**
  Tell them the phone with your banking apps and mobile wallet was stolen. Ask them to watch for unusual transfers and new payees.

- [ ] **Change your Apple Account or Google Account password**
  Review the email addresses, phone numbers and recovery methods on the account, and remove the stolen phone from the trusted device list without removing it from Find My.

- [ ] **Change passwords on banking, payment and investment apps**
  Then move to social media, shopping and cloud storage accounts. Use unique passwords from a password manager.

- [ ] **Find the IMEI and serial number without the phone**
  For an iPhone, sign in at account.apple.com and open Devices. For Android, open Settings in Find Hub. The original box also carries both numbers.

- [ ] **File a police report and include the IMEI and serial number**
  Give the time, place and any location shown on the map. Keep the report number for your carrier, insurer and bank.

- [ ] **Watch for messages claiming your phone has been found**
  Apple says it will never contact you to say your device was found. Messages like this are often phishing attempts to get your passcode or account password.

This week

- [ ] **Erase the phone remotely once you give up on recovery**
  Erasing cannot be undone. A recent iPhone can still be located after erasing; an Android phone no longer appears in Find Hub after a factory reset.

- [ ] **File an insurance or device protection claim if you have coverage**
  Check your carrier plan, AppleCare+ with Theft and Loss, card benefits, or renters or homeowners policy. Terms, deductibles and deadlines vary by policy.

- [ ] **Review account activity for logins and changes you did not make**
  Check email, banking, payment apps and social media for new devices, changed recovery details and messages sent in your name. See our hacked account guide (confirmedstolen.com/hacked-accounts/).

- [ ] **Report identity theft if new accounts were opened**
  If someone used information from the phone to open accounts, create a recovery plan at IdentityTheft.gov (www.identitytheft.gov/).

Prevent it happening again

- [ ] **Turn on Stolen Device Protection or Android theft protection**
  On an iPhone, look under Settings, Face ID and Passcode. On Android, look under Settings, Google, All services, Theft protection.

- [ ] **Use a strong device passcode and guard it in public**
  A long passcode is harder to watch over your shoulder. Never share it, or any verification code, with anyone who contacts you.

- [ ] **Move multi-factor authentication off text messages**
  Use an authenticator app, a hardware security key or a passkey on email, banking and other high-value accounts.

- [ ] **Record your IMEI and serial number somewhere safe today**
  Keep them in a password manager or with your important papers so you can give them to police and your carrier without delay.

Your case record

Phone make, model and IMEI

Carrier case number

Police report number

Insurance or protection plan claim number

Accounts secured (date)

Notes

Version November 6, 2026. General information, not legal advice. Agencies change their procedures, so confirm each step with the organization named. Confirmed Stolen is an independent reference; it is not law enforcement and does not recover property. Free to print and share with attribution.