PERSONAL PRIVACY GUIDE

# Personal Privacy & Secure Phone Planning Guide

A plain-language plan for choosing a secure phone, locking down your accounts, controlling location sharing, and keeping your communications private, for yourself and your family.

**For:** Individuals and families **Edition:** November 2026 **Web:** spmadvisors.net

## ABOUT SPM ADVISORS

Veteran-owned cybersecurity and digital forensics firm helping organizations, healthcare practices, and individuals understand their risk and respond when something goes wrong. Learn more at spmadvisors.net.

## INSIDE THIS GUIDE


1. Choosing a secure phone
2. Account privacy
3. Location sharing
4. Private communications
5. Planning for families
6. Preparation checklist
7. Tracking, abuse, and evidence

**READ THIS FIRST IF YOU MAY BE TRACKED OR MONITORED**

If you think someone you know is monitoring your phone, accounts, or location, **read Tracking, abuse, and evidence before changing anything.** Removing apps, changing passwords, or turning off sharing can alert the other person and may increase risk. It can also destroy evidence you may need later. Plan with a trained advocate first, using a device the other person has never had access to.

If you are in immediate danger, call 911.

# Choosing a secure phone

A secure phone starts with where it came from and how long it will keep receiving security updates. Brand matters less than keeping the device current and under your sole control.

### Selection

- **Buy new, from the manufacturer or carrier.** Avoid used phones, or phones given to you by someone who may have had access to them.
- **Check the update commitment.** Choose a current model with years of guaranteed security updates remaining. Manufacturers publish these dates.
- **Retire unsupported phones.** A phone that no longer receives security updates should not hold your primary accounts.

### Initial setup

- Use a passcode of at least six digits, or an alphanumeric passcode. Avoid birthdays and patterns.
- Turn on automatic software updates.
- Install apps only from the official app store, and only the ones you need.
- Hide notification content on the lock screen.

## Built-in protections worth knowing

### Platform security features

| FEATURE | PLATFORM | WHAT IT DOES |
|---|---|---|
| Stolen Device Protection | iPhone | Requires Face ID or Touch ID, and adds a delay, before sensitive changes such as your Apple Account password when away from familiar locations. |
| Theft protection | Android | Locks the screen when a phone appears to be snatched or goes offline, and adds identity checks for sensitive settings. |
| Safety Check | iPhone | Reviews and resets which people and apps have access to your location, photos, and other information. |
| Lockdown Mode / Advanced Protection | iPhone / Android | Optional high-security modes for people at elevated risk of targeted attack. They limit some features in exchange for stronger protection. |

**PROTECT YOUR PHONE NUMBER**

Ask your carrier to add an account PIN and turn on number-lock or port-out protection. This makes it harder for someone to move your number to their own device (a "SIM swap") and intercept your text-message codes.

## Account privacy

Your Apple Account or Google Account is the master key to your phone: backups, photos, messages, location history, and passwords often flow through it. Secure it first.

- **Use a unique password** stored in a password manager. Where offered, switch to passkeys.
- **Turn on two-step verification** using an authenticator app, passkey, or hardware security key rather than text messages where possible.
- **Check recovery options.** Your recovery email, phone number, and trusted contacts should belong only to you or people you fully trust.
- **Review signed-in devices** and remove any you do not recognize or no longer use.
- **Review connected apps** and third-party access, and remove what you do not use.
- **Check email settings** for forwarding rules or filters you did not create.
- **Secure the second tier:** email, banking, mobile carrier, social media, and cloud storage accounts.

## Location sharing

Location can be shared in more places than most people realize. Review each one and decide deliberately who should see where you are.

### Where location is shared

- Find My (Apple) and Find Hub (Google)
- Google Maps location sharing
- Family locator apps such as Life360
- Social apps (for example, Snap Map) and check-ins
- Connected car apps and smart home accounts
- Fitness apps and shared activity maps
- Photo metadata when sharing pictures

### What to do

- Review location permissions app by app; choose "while using" or "never" where possible
- Turn off precise location for apps that do not need it
- Remove people you no longer want to share with, after considering safety
- Pay attention to unknown-tracker alerts. Both iPhone and Android can warn you about a Bluetooth tracker traveling with you

## Private communications

- **Use end-to-end encrypted messaging** for sensitive conversations. Signal is a strong default. iMessage and WhatsApp are also end-to-end encrypted. Standard SMS text messages are not.
- **Use disappearing messages** for conversations that do not need to be kept, but see the evidence guidance below before deleting anything related to harassment or abuse.
- **Remember backups.** Messages may be copied to cloud backups. On iPhone, Advanced Data Protection extends end-to-end encryption to most iCloud data.
- **Treat email as less private.** Avoid sending sensitive documents by ordinary email when a secure alternative exists.

- **Verify unexpected requests.** Scammers impersonate banks, family members, and even voices. Hang up and call back on a number you already know.

## Planning for families

### Children and teens

- Use built-in parental controls openly, and explain them
- Know which accounts and apps your child uses
- Agree on rules for sharing photos and location
- Revisit settings as children get older

### Shared and changing households

- Review Family Sharing and shared cloud accounts
- Know who can see shared photo albums and calendars
- When a household changes, review all shared access
- Help older relatives set up scam protections

## Preparation checklist

Work through this list at your own pace. If tracking or abuse may be involved, complete the safety section first and plan changes with an advocate.

### Before you start

- [ ] Make a list of your important accounts (email, phone carrier, banking, cloud, social)
- [ ] Set up a password manager
- [ ] Note which devices are signed in to each account
- [ ] Write down who you currently share location with

### Phone

- [ ] Phone is current and receiving security updates
- [ ] Strong passcode set; automatic updates on
- [ ] Stolen Device Protection or theft protection on
- [ ] Carrier account PIN and number-lock set
- [ ] Unused apps removed

### Accounts

- [ ] Unique passwords or passkeys on key accounts
- [ ] Two-step verification on with an app or key
- [ ] Recovery email and phone confirmed as yours
- [ ] Unknown devices and connected apps removed
- [ ] Email forwarding rules checked

### Location and communications

- [ ] Location permissions reviewed app by app
- [ ] Sharing list reviewed in each location app
- [ ] Encrypted messaging set up for sensitive contacts
- [ ] Lock screen previews hidden
- [ ] Cloud backup encryption reviewed

### Family

- [ ] Family Sharing and shared accounts reviewed
- [ ] Children's controls set and explained
- [ ] Family "call-back" rule agreed for urgent money requests

### Keep it current

- [ ] Repeat this review every three months
- [ ] Review again after a new phone, a move, or a relationship change
- [ ] Re-check after any suspicious login alert

## Tracking, abuse, and evidence

Technology is often misused in stalking and domestic abuse. If that may be part of your situation, safety comes before privacy settings. The steps below are general cautions, not a substitute for a safety plan built with a trained advocate.

> **CHANGES CAN ALERT THE OTHER PERSON**
>
> Removing a monitoring app, changing a password, or turning off location sharing may be noticed right away. If the person is controlling or dangerous, a sudden change can escalate risk. Talk with an advocate about timing before you act.

### Use a safer device to get help

If your phone or computer may be monitored, research and contact help from a device the other person has never had access to: a trusted friend's phone, a library computer, or a new phone on a new account.

### Preserve before you delete

- **Document first.** Take screenshots of messages, alerts, and suspicious settings. Photograph the screen with another device when screenshots could be noticed.
- **Keep a log** of incidents: date, time, what happened, and how you think the person knew what they knew.
- **Do not factory-reset or discard a device** you may need as evidence until you have spoken with an advocate, attorney, or law enforcement. A reset can erase the proof.
- **If you get an unknown-tracker alert,** do not simply throw the tracker away. Note what the alert shows, and contact law enforcement or an advocate about preserving it safely.
- **Store copies safely** in an account or location the other person cannot reach.

### Signs that may suggest monitoring

Someone knows where you have been or what you said privately; you see unfamiliar apps, profiles, or device management settings; or you receive login alerts or password reset emails you did not request. These signs do not prove monitoring, and monitoring does not always produce signs. A consent-based examination by a qualified forensic professional can help confirm what is happening.

**STAY ON THE RIGHT SIDE OF THE LAW**

Do not log in to, install software on, or track another person's device or accounts, even to gather evidence. That can be illegal and can harm your case. Questions about shared devices, children's phones in custody situations, or accounts in someone else's name should go to an attorney.

**WHERE TO GET HELP**

- **Emergency:** call 911.
- **National Domestic Violence Hotline:** 1-800-799-7233, or text START to 88788 (thehotline.org).
- **Safety Net Project (NNEDV):** technology safety resources at techsafety.org.
- **Coalition Against Stalkerware:** stopstalkerware.org.
- **Stalking Prevention, Awareness, and Resource Center (SPARC):** stalkingawareness.org.

This guide provides general information for planning purposes. It is not legal advice and does not create a client relationship. Requirements and product features change; confirm current details before relying on them. © 2026 SPM Advisors LLC. Edition: November 2026.