Safer in a Digital World

Practical Tech Safety for Advocates

Start with safety, not the device.

Digital threats require digital safety strategies.

Start the Conversation

1. What accounts and platforms do you use?
2. What's the safest way for us to communicate
3. Does anyone know your passwords or see your location?
4. Who set up, pays for, or can access your devices?
5. Does someone seem to know things they shouldn't?

Check Access First

Shared accounts are often the #1 threat.

- Known or shared passwords
- Family plans and kids' devices on an abuser's account
- Location sharing (Find My, Google)
- Shared photo streams and cloud backups
- Apple Safety Check or Google Security Checkup

Watch the Digital Trail

What digital traces does this leave?

- Notifications and call logs
- Browser history and linked devices
- Keyboard suggestions and app switcher
- Backups and shared cloud copies
- Secure apps need setup too: disappearing messages, app lock

Tracking and Surveillance

Detect → Document → Decide → Safety Plan

- Don't automatically destroy trackers, make a plan first
- If the survivor wants to, they can consider photographing it and record serial numbers.
- Disabling a tracker or ending an account session can alert the abuser.

Common tracker types: Bluetooth trackers • GPS trackers • the phone itself

Preserve Evidence Safely

- Screenshot the whole screen: sender, date, time
- Keep the original untouched; annotate a copy
- Keep a simple log: date, time, what happened
- Store copies where the abuser can't reach
- A shared cloud folder may notify the abuser

When Images Are Involved

Platforms must remove reported intimate images within 48 hours.

Request ignored? **TakeItDown.ftc.gov**

Image taken at 18 or older: **StopNCII.org**

Image taken under 18: **NCMEC Take It Down**

On the Agency Side

- Dedicated agency devices, number, and social media accounts
- Plan for safer methods for contact
- Document in agency records, not the app
- Only use channels the survivor approves

1 Never touch a client's phone.

Not if they ask. Not if you could do it faster. Teach them what to do. Don't do it for them.

2 No guarantees of safety.

Never say a device, app, or account is "safe." A determined abuser has many paths to tech-facilitated abuse..

Scan for the full handout and tech-safety resources

SocialStrategies.com/i/techsafety.pdf

Technology changes quickly. Current as of Fall 2026

SOCIAL STRATEGIES
Transforming. Together.