Protect Devices and Browsing

- ■ Install operating-system, browser, and app updates
- ■ Use a strong screen lock and device encryption
- ■ Enable device finding, remote locking, and remote erase
- ■ Audit location, camera, microphone, contacts, photos, and file permissions
- ■ Remove unused apps, browser extensions, and connected services
- ■ Review live-location and family-location sharing
- ■ Review advertising ID and ad-privacy controls
- ■ Block third-party cookies and trackers where practical
- ■ Remove photo location metadata before sensitive posts

Prepare for Harassment or Doxxing

- ■ Write down who I will contact
- ■ Identify someone who can monitor and document abuse
- ■ Know how to make accounts private quickly
- ■ Create a secure evidence folder and incident log
- ■ Decide when to contact a platform, employer, school, attorney, advocate, or emergency service
- ■ Make a household communication and safety plan
- ■ Keep a copy of the plan outside my primary account

If I Suspect Stalkerware

- ■ Use a safer device and make a safety plan before changing settings or passwords

Maintain

- ■ Search my name and contact details monthly
- ■ Review privacy settings and app permissions quarterly
- ■ Recheck broker removals
- ■ Review active sessions and connected apps
- ■ Update my response plan annually
- ■ Repeat the review after a move, new public role, threat, breach, or lost device

“Complete privacy is rarely possible. The goal is to reduce unnecessary exposure, make misuse harder, and be prepared to respond.”
