

# iOS Security Features You Should Know

## Auto-Restart After 3 Days (NEW!)

If your iPhone isn't unlocked for 3 days, it automatically restarts. This puts it in a "Before First Unlock" state—the most secure mode possible. Great for seized or stolen devices.

## Stolen Device Protection

- Requires Face ID or Touch ID for critical changes when away from home/work
- Adds 1-hour delay before disabling Find My or changing passwords
- Gives you time to mark device as lost

## Lockdown Mode

- Extreme protection for high-risk individuals
- Blocks most attachments and link previews
- Disables FaceTime calls from unknown numbers
- Limits JavaScript and fonts

Enable these in: Settings → Privacy & Security



# Action Items: Start Today

Pick 3-5 items to implement this week:

1. Enable 2FA on your most important accounts
2. Install Privacy Badger or AdGuard
3. Review phone app permissions
4. Review and adjust your Meta/Facebook privacy settings (quarterly)
5. Switch to DuckDuckGo as your default search engine
6. Test your browser at [coveryourtracks.eff.org](https://coveryourtracks.eff.org)
7. Disable ad tracking on your phone
8. Start using a password manager
9. Use disposable/randomized remailer addresses when creating accounts
10. Cover your webcam
11. Enable auto-restart and Stolen Device Protection
12. Disable biometric unlock at borders
13. Cut back Google dependence
14. Reboot your devices weekly (daily when traveling)