



SMARTPHONE SAFETY CHECKUP

Plain-language settings for safer iPhone and Android use

START WITH THESE SIX PROTECTIONS

Menu names vary by model and software version

- 1 Lock the phone**
Strong PIN plus face or fingerprint unlock.
- 2 Install updates**
Keep the system, patches and apps current.
- 3 Screen contacts**
Filter unknown calls and messages.
- 4 Protect apps**
Keep web warnings and app scanning on.
- 5 Secure accounts**
Use two-factor authentication or a passkey.
- 6 Prepare for theft**
Enable theft protection and device finding.

i APPLE IPHONE - RECOMMENDED SETTINGS

- 1 Automatic security updates**
Settings > General > Software Update > Automatic Updates
Turn on automatic installation. Updates can install overnight while charging on Wi-Fi.

- 5 Separate unknown messages**
Settings > Apps > Messages > Unknown Senders
Turn on Screen Unknown Senders. Older phones may call this Filter Unknown Senders.

- 2 Strong passcode and Face ID or Touch ID**
Settings > Face ID & Passcode
Use at least six digits. Enroll only your own face or fingerprints.

- 6 Safari safety warnings**
Settings > Apps > Safari > Privacy & Security
Turn on Fraudulent Website Warning and Block Pop-ups. Leave any warned page.

- 3 Stolen Device Protection**
Settings > Face ID & Passcode > Stolen Device Protection
Turn it on. Choose Always for the security delay when that option is available.

- 7 Hide Lock Screen previews**
Settings > Notifications > Show Previews
Choose When Unlocked so messages, alerts and verification codes stay hidden.

- 4 Screen unknown callers**
Settings > Apps > Phone > Screen Unknown Callers
Use Ask Reason for Calling when available. Save trusted numbers in Contacts first.

- 8 Apple Account two-factor authentication**
Settings > your name > Sign-In & Security
Confirm it is on and your trusted number is current. Never share a sign-in code.



SMARTPHONE SAFETY CHECKUP

Android settings and what to do when something suspicious gets through

A ANDROID PHONES - RECOMMENDED SETTINGS

- 1 Security & privacy checkup**
Settings > Security & privacy
Review every warning and recommendation for the device, apps and account.
- 2 Strong screen lock and biometrics**
Settings > Security & privacy > Device lock
Use a PIN of at least six digits. Avoid birthdays and repeating numbers.
- 3 Android and security updates**
Settings > System > Software updates
Install operating-system, security and Google Play system updates.
- 4 Caller ID and spam filtering**
Phone > menu > Settings > Caller ID & spam
Turn on caller ID and spam protection. Enable call screening where offered.
- 5 Message spam protection**
Google Messages > profile > Messages settings > Protection & Safety
Keep spam protection on. The option may differ by device or messaging app.
- 6 Google Play Protect**
Play Store > profile > Play Protect > Settings
Turn on app scanning and harmful-app detection. Use only trusted app stores.
- 7 Theft protection**
Settings > Google > All services > Theft protection
Enable supported theft, offline, failed-authentication and remote locks.
- 8 Chrome Safety Check**
Chrome > menu > Settings > Safety check
Correct every issue. Enable secure connections and breach warnings where offered.
- 9 Hide sensitive notifications**
Settings > Notifications > Notifications on lock screen
Hide sensitive content so messages and codes are not visible while locked.
- 10 Google 2-Step Verification**
Google Account > Security & sign-in > 2-Step Verification
Turn it on and consider a passkey. Approve only sign-ins you started.

IF SOMETHING SUSPICIOUS GETS THROUGH

- Do not click, reply, install an app, or share a passcode or verification code.
- Hang up and contact the organization using a number you find independently.
- Never move money to protect it or keep a transaction secret.



FULL STEP-BY-STEP GUIDE
TNElderJusticeCoalition.org

Settings are a safety net, not proof that a contact is legitimate.