



FAMILY CYBER-HARDENING GUIDE

COMPLETE GUIDE • Companion to the Action Plan

START HERE FIRST The Action Plan tells you what to do. The Complete Guide tells you exactly how.

How to use this guide

You are not expected to complete every page today. Return here when you are ready to secure one area, need an exact settings path, or want help with a specific account.

1 START HERE	2 CHOOSE A MODULE	3 GET HELP IF NEEDED
Use the four-page Action Plan and complete the five protections marked “today.”	Pick the section that matters now. Each module restarts at Step 1 and can be completed independently.	Schedule a 30-minute family setup session or ask a trusted helper to walk through one module with you.

Choose what you need next

Protect the essentials: iPhone • Apple Account • Email • Passwords and passkeys

Protect money and identity: Banking and investments • Cellular/SIM • Credit freezes

Protect everyday activity: Browsers • Shopping and social media • Home Wi-Fi • Backups

Prepare the family: Voice-clone protocol • Safe AI agents • Incident response

Optional advanced protection: Security keys • Apple/ChatGPT Lockdown Mode • Advanced Data Protection

OUR FAMILY’S FIVE NON-NEGOTIABLE RULES 1) Never share a code, passkey prompt, or recovery secret with anyone who contacted you; never approve a sign-in you did not start. 2) Never move money to a ‘safe’ account. 3) Never install remote-access software because of an inbound contact. 4) Never send urgent money based only on an inbound call or message—even if the voice or video looks real. 5) Independently contact the person or company before acting.

ONE MODULE AT A TIME • Each section is independent; every module restarts at Step 1.

When something feels wrong: STOP → HANG UP → CALL BACK using a number you already trust → VERIFY → THEN ACT.

Keep this kit current

LAYER	REVIEW WHEN	WHY
Five rules + callback	Yearly or after an incident	The human protocol changes slowly.
Settings + recovery	Every major OS/app release	Labels, defaults, and recovery options drift.
AI connectors	Every quarter	Permissions and connected capabilities change quickly.

IF THIS HOUSEHOLD INCLUDES...

CHILD / TEEN — APPLE Use a Child Apple Account, Family Sharing, Communication Safety, Ask to Browse when available, unique school/gaming credentials, and minor freezes. Communication Safety does not send message contents to parents.

TEEN AI Use ChatGPT parental controls as one layer. Parents cannot see ChatGPT conversation transcripts.

AGING PARENT Set this up with permission, rehearse the callback rule, and document the bank trusted contact or verbal password and appropriate legal authority.

ANDROID OR WINDOWS This Apple-first kit’s update, lock, passkey, carrier, alert, backup, and callback rules still apply; use provider instructions.



Why act now—without panicking

AI lowers the cost of creating personalized phishing, cloned voices, realistic documents, and automated attacks. The good news is that the strongest defenses are ordinary, available now, and mostly one-time setup: updates, unique credentials, sign-in that a fake site cannot capture, alerts, recovery planning, and independent verification.

A SIMPLE RULE Treat urgency, secrecy, and requests for money or codes as a reason to slow down—not speed up.

Priority map

WHEN	FOCUS	GOAL
Today	Updates; phone passcode; stolen-device protection; Apple/email 2FA; bank alerts	Stop the fastest account takeovers
This week	Password cleanup; passkeys; carrier lock; router; freezes; backups; family drill	Break the chain between one mistake and total loss
Advanced	Two hardware security keys; separate financial email; Apple/ChatGPT Lockdown Mode for higher-risk people	Reduce targeted and agent-related risk

1. iPhone: lock the front door

WHY IT MATTERS A stolen phone plus a known passcode can expose passwords, email, and money. Updates close known holes.

- ☐ Settings → General → Software Update. Install the current point release today, even if Automatic Updates is on. Then open Automatic Updates and confirm downloads and installations are enabled.
- ☐ Settings → Face ID & Passcode (or Touch ID & Passcode). Use a unique passcode of at least 6 digits; choose Passcode Options for a longer numeric or alphanumeric code. Do not use birthdays or address numbers.
- ☐ On that same screen, review “Allow Access When Locked.” Turn off anything you would not want a stranger to use from the lock screen. Keeping Control Center off can make it harder to disable connectivity; decide based on convenience.
- ☐ Settings → Face ID & Passcode → Stolen Device Protection. On iOS 26.4 or later, Apple automatically enables it for new setups and restores, and when a device running 26.4 updates to a later iOS version; still confirm it is on.
- ☐ Confirm the prerequisite chain: device passcode; Face ID or Touch ID; Apple Account two-factor authentication; Find My; and Settings → Privacy & Security → Location Services → System Services → Significant Locations & Routes.
- ☐ Under Require Security Delay, “Always” gives more protection; “Away from Familiar Locations” is the easier default.
- ☐ Lock Mail and sensitive financial apps: on the Home Screen, touch and hold the app, then tap Require Face ID (or Touch ID). With Stolen Device Protection, a locked app can require biometrics without passcode fallback away from familiar locations.



8. ☐ Settings → [your name] → Find My → Find My iPhone. Turn on Find My iPhone, Find My network, and Send Last Location.
9. ☐ Settings → Privacy & Security → Tracking → turn off Allow Apps to Request to Track. This is privacy—not a substitute for account security.

Menu labels verified against Apple's iOS 26 guides in August 2026; older iOS versions may differ.

MODULE COMPLETE ☐ Date: _____

2. App permissions: give less access

WHY IT MATTERS An app cannot leak or misuse data it was never allowed to collect.

1. ☐ Settings → Privacy & Security. Open Location Services, Contacts, Calendars, Photos, Bluetooth, Local Network, Microphone, Camera, and Motion & Fitness one at a time.
2. ☐ Remove access from apps that do not clearly need it. For location, prefer Never or While Using; turn Precise Location off when approximate location is enough.
3. ☐ For Photos, choose limited access when the app needs only a few pictures. For Contacts, share only selected contacts when the option is available.
4. ☐ Delete apps you no longer use. Review again every six months and after installing a major new app.

Do not use Safety Check as a routine “cleanup” button. It is designed especially for quickly reviewing or stopping sharing with people and apps: Settings → Privacy & Security → Safety Check.

MODULE COMPLETE ☐ Date: _____

3. Apple Account and recovery

WHY IT MATTERS Your Apple Account can unlock backups, passwords, photos, messages, and device recovery.

1. ☐ Settings → [your name] → Sign-In & Security. Confirm Two-Factor Authentication is on and the trusted phone numbers are current.
2. ☐ On the Apple Account screen, scroll through devices. Tap and remove any device you no longer own or recognize.
3. ☐ Settings → [your name] → Sign-In & Security → Recovery Contacts. Add one or more trusted people who can help you regain access. A recovery contact cannot see your data.

△ ADVANCED — ASK FOR HELP IF UNSURE Advanced Data Protection and physical security keys strengthen protection but make recovery planning essential.

4. ☐ Advanced Data Protection: Settings → [your name] → iCloud → Advanced Data Protection. Read Apple's recovery warning first; you become responsible for account recovery.
5. ☐ Physical security keys: Settings → [your name] → Sign-In & Security → Two-Factor Authentication → Security Keys. Register at least two compatible FIDO keys (small physical sign-in devices) and keep the spare separately.

MODULE COMPLETE ☐ Date: _____



4. Email: protect the master key

WHY IT MATTERS Password resets for nearly every other account arrive by email.

1. ☐ In your email provider's Security settings, change any reused password to a unique password saved in your password manager.
2. ☐ Turn on two-step verification. Choose a passkey or security key when available; otherwise use an authenticator app. Use text messages only when stronger choices are unavailable.
3. ☐ Review signed-in devices, recent security activity, forwarding rules, filters, delegates, connected apps, recovery email, and recovery phone. Remove anything unfamiliar or old.
4. ☐ Save recovery codes offline in a secure place. Never send them by email or text.
5. ☐ After testing passkeys, security keys, recovery codes, and recovery contacts, remove SMS as a sign-in or recovery fallback wherever the provider permits. Do not remove a required recovery number until another recovery path is tested.
6. ☐ Consider a private, separate email address used only for financial accounts and account recovery. Do not publish it or use it for shopping.

MODULE COMPLETE ☐ Date: _____

5. Passwords, passkeys, and security keys

THE ORDER TO PREFER Passkey (a safer replacement for a password) or hardware security key → authenticator app → text-message code → password alone. Never approve a sign-in you did not start.

1. ☐ Choose one trusted password manager and protect it with a strong, memorable master password or device passkey (a safer replacement for a password). On iPhone, Apple's Passwords app is built in.
2. ☐ Settings → General → AutoFill & Passwords → turn on AutoFill Passwords and Passkeys; select only the password manager(s) you actually use.
3. ☐ Fix reused passwords first. Priority: email, Apple Account, carrier, bank, brokerage, payment apps, social media, cloud storage, health portals.
4. ☐ When a service offers "Create a passkey," accept it. A passkey is tied to the real website/app and is much harder to phish.
5. ☐ Know where the passkey lives. Most iPhone passkeys sync through iCloud Keychain for convenience; a passkey saved to a hardware security key stays on that physical key. Both resist fake websites, but recovery is different—document the recovery plan.

△ ADVANCED — ASK FOR HELP IF UNSURE Physical security keys are excellent protection, but losing every enrolled key can complicate recovery.

6. ☐ For hardware keys, buy two compatible FIDO2 keys (FIDO2 is a phishing-resistant security-key standard): primary plus backup. Enroll both before relying on them; label without naming the account; store separately.

TEST BEFORE REMOVING SMS Sign in with each enrolled key and test the written recovery plan before removing an SMS fallback anywhere.



NEVER SHARE A legitimate support person should not ask for your password, passkey, one-time code, recovery code, recovery key, screen-sharing control, or a transfer to a “safe” account.

MODULE COMPLETE ☐ Date: _____

6. Banking, investing, and payment apps

WHY IT MATTERS Strong sign-in helps; transaction controls and human verification limit damage if something still goes wrong.

1. ☐ Use the official app or a bookmark you created—not a link in a message, search ad, QR code, or unexpected pop-up.
2. ☐ In Profile/Settings → Security (wording varies), enable the strongest sign-in offered: passkey/security key first, authenticator app next. Add biometric app lock if offered.
3. ☐ After stronger sign-in and recovery are tested, remove SMS as a login or account-recovery fallback wherever the institution allows it. Keep current contact information for legitimate fraud alerts.
4. ☐ In Alerts/Notifications, turn on: every transaction or threshold you care about; login/new device; password/profile change; new payee; external account link; wire/ACH transfer; card-not-present purchase; cash withdrawal.
5. ☐ Set transfer and card limits as low as practical. Lock unused debit cards. Consider disabling wire transfers until needed.
6. ☐ Use a unique private financial email and, if supported, a verbal password for phone service. Ask the institution to note that no instruction is valid solely by email, text, or an inbound call.
7. ☐ Never let an AI agent autonomously trade, move money, add payees, change beneficiaries, or handle tax/payment details. Use AI for research or drafting; you independently verify and execute consequential actions in the official app.

Investment values can change quickly; verify any AI-generated quote, holding, tax statement, or recommendation against the brokerage's official records. AI output is not authorization.

MODULE COMPLETE ☐ Date: _____

7. Cellular, eSIM, and port-out protection

WHY IT MATTERS A SIM swap, eSIM transfer, or port-out can move your phone number to another device or carrier and redirect calls and text-message security codes.

1. ☐ Call your carrier using the number on its official site or bill. Add a strong account PIN/passcode that is not your phone passcode.
2. ☐ Ask for a port-out lock, number lock, or SIM-swap protection. Ask what verification is required to transfer an eSIM to a new phone and what must happen before any lock can be removed.
3. ☐ Secure the carrier's online account with a unique password and strongest MFA available. Remove old authorized users and lines.
4. ☐ If the carrier allows a passkey or authenticator plus non-SMS recovery, use it and remove SMS as a fallback. Some carriers still require the phone number, so confirm recovery before changing anything.



⚠ **ADVANCED — ASK FOR HELP IF UNSURE** A device SIM PIN can lock the SIM after wrong attempts and may require a carrier recovery code.

5. ☐ Optional device SIM PIN: Settings → Cellular → SIM PIN. Set a PIN you can reliably store. Warning: too many wrong attempts can lock the SIM and require the carrier's PUK code.

MODULE COMPLETE ☐ Date: _____

8. Browsers and safer links

WHY IT MATTERS Convincing fake login pages are common. Passkeys help, but your habits still matter.

1. ☐ Safari: Settings → Apps → Safari. Turn on Prevent Cross-Site Tracking. Under Hide IP Address, choose Trackers Only; with iCloud+ Private Relay, Trackers and Websites is stronger. If one site breaks, temporarily allow that site rather than disabling protection globally.
2. ☐ For Chrome, Edge, Firefox, or another browser, enable automatic updates, built-in safe-browsing/protection, and HTTPS-only mode if offered. Review extensions and delete any you do not need.
3. ☐ Do not install a browser extension because a caller, pop-up, or “support technician” tells you to. Extensions can read pages and sometimes sensitive data.
4. ☐ For email, bank, carrier, Apple, and investment logins, open the official app or your saved bookmark. If a message claims there is a problem, do not use its link or phone number.

MODULE COMPLETE ☐ Date: _____

9. Everyday online safety: shop, scroll, and connect

THE FAMILY RULE See it in a feed → leave the feed → open the official app or site → verify → then decide.

AI can create convincing ads, stores, reviews, profiles, recruiters, and customer support. Verify independently before you buy, reply, apply, invest, or share.

1. ☐ Treat every ad as an introduction—not an endorsement. Social platforms, search engines, and influencers may display ads from scammers or brand impersonators.
2. ☐ Do not use an unexpected QR code on a parking meter, invoice, sign, email, text, or package for login or payment. Open the official app or known website instead; a QR code hides its destination until scanned.
3. ☐ Do not buy through a social-media ad link. Open the retailer's official app, use your bookmark, or type the known address. Do the same for delivery, refund, account-warning, and support messages.
4. ☐ For an unfamiliar seller, search its name plus “scam,” “complaint,” and “reviews.” Check independent sources, contact details, return terms, and unrealistic prices. A padlock or https does not prove honesty.
5. ☐ Prefer a credit card or protected checkout. Avoid debit cards, wires, cryptocurrency, gift cards, checks, and payment-app “friends and family” transfers for unfamiliar purchases.
6. ☐ On Amazon or another marketplace, check who sells and ships the item, seller history, recent detailed reviews, return terms, and whether the listing changed products. Keep payment and messages in the platform.
7. ☐ Do not trust reviews, follower counts, photos, voices, videos, testimonials, or verification-looking graphics alone. AI can fabricate them. Confirm important claims outside the post or message.
8. ☐ On TikTok, Instagram, Facebook, and similar apps, limit who can see your location, birthday, relatives, travel plans, school, workplace, contacts, and routines. These details help personalize scams.



9. ☐ For LinkedIn or job sites, confirm the role on the employer's official careers page. Prefer verified profiles and company-domain email, but verify independently. Never pay for equipment or send banking, SSN, or ID documents before a legitimate offer and secure onboarding.
10. ☐ Never let a seller, recruiter, influencer, "support agent," or online acquaintance persuade you to install remote-access software, an extension, app, or configuration profile—or move money to a "safe" account.
11. ☐ Treat investment, romance, giveaway, charity, and "easy income" messages as high-risk when they start on social media or move to a private channel. Stop at secrecy, urgency, guaranteed returns, or payment.

THE SLOW-TRUST RULE Weeks of friendly chat, photos, calls, or video do not prove identity. A new relationship that moves off-platform and then toward investing, cryptocurrency, "recovery help," money, or secrecy is a stop.

WHEN IN DOUBT Take a screenshot, close the app, and ask a trusted person. Missing a sale or opportunity is cheaper than reversing fraud.

MODULE COMPLETE ☐ Date: _____

10. Home Wi-Fi and router

WHY IT MATTERS The router sits between every home device and the internet.

1. ☐ Open the router maker's official app or type the router address printed in its manual. Install firmware updates and enable automatic updates if available.
2. ☐ Change the router administrator password. It must be unique and different from the Wi-Fi password. Disable remote administration unless you truly need it.
3. ☐ Use WPA3 Personal if every device supports it; otherwise WPA2/WPA3 transition mode or WPA2-AES (modern encrypted Wi-Fi). Do not use WEP or open Wi-Fi.
4. ☐ Use a long, unique Wi-Fi passphrase. Rename the network so it does not reveal your family name, address, or router model.
5. ☐ Create a guest network for visitors and, if practical, internet-connected devices such as cameras, TVs, plugs, and appliances.

△ ADVANCED — ASK FOR HELP IF UNSURE Disable WPS and UPnP (automatic device port-opening) only after confirming your devices do not depend on them.

6. ☐ If confirmed unnecessary, disable WPS and UPnP in the router's advanced settings.
7. ☐ Replace a router that no longer receives security updates. Record the model and check the maker's support page yearly.

MODULE COMPLETE ☐ Date: _____

11. Credit freezes

WHY IT MATTERS A freeze makes it harder for an identity thief to open new credit in your name. It does not affect your credit score and can be lifted when needed.

1. ☐ Freeze separately with all three bureaus using only their official sites: Equifax.com, Experian.com, and TransUnion.com. Freezes are free under U.S. law.



2. ☐ Create unique credentials for each bureau and protect them with MFA when offered. Save confirmation and recovery information in your password manager or secure offline records.
3. ☐ For a child under 16, a parent or legal guardian requests a freeze at each bureau using its minor-freeze process and extra documents. Minors age 16 or 17 may request and remove their own freeze. Consider Innovis and a ChexSystems security freeze for added coverage.
4. ☐ Check credit reports at AnnualCreditReport.com. If identity theft occurs, use IdentityTheft.gov for a recovery plan.
5. ☐ Request a free IRS Identity Protection PIN at IRS.gov/IPPIN for each eligible taxpayer and dependent. For a dependent under 18, follow the IRS alternative-enrollment instructions. A new IP PIN is generated yearly; the IRS will not call, email, or text to ask for it.
6. ☐ Claim USPS Informed Delivery at informedelivery.usps.com so your household controls the account. Consider OptOutPrescreen.com to reduce prescreened credit and insurance offers.

A credit freeze mainly blocks new-credit accounts. It does not stop takeover of an existing bank or card account, tax-refund fraud, or medical identity theft; keep account alerts and the IRS IP PIN.

MODULE COMPLETE ☐ Date: _____

12. Backups and recovery

WHY IT MATTERS A backup turns theft, loss, ransomware, or a bad update into an inconvenience instead of a family disaster.

1. ☐ iPhone: Settings → [your name] → iCloud → iCloud Backup → turn on Back Up This iPhone. Tap Back Up Now and confirm a recent successful backup.
2. ☐ For computers, use automatic backup software. Keep at least one second copy that is not always attached to the computer—an encrypted external drive stored safely or a reputable cloud backup.
3. ☐ Once every few months, open a few backed-up files or photos and confirm they restore. A backup that has never been tested is only a hope.
4. ☐ Keep a paper or offline recovery sheet: key contacts, carrier, banks, Apple/email recovery method, device serial numbers, and where the password-manager emergency instructions, backup, and security keys are stored. Record the location of the master-password instructions—not the password itself. Never write one-time codes.

MODULE COMPLETE ☐ Date: _____

13. Family voice-clone and scam protocol

THE FAMILY RULE No urgent request for money, credentials, codes, secrecy, or remote access is acted on during the original contact—even when the voice or video looks real.

1. ☐ Pause. Say: “I’m going to verify this and call you back.” Hang up.
2. ☐ Call the person using a number already stored in your contacts. If unavailable, call a second trusted family member.
3. ☐ Use a challenge or two-part family phrase that is not posted online. Never speak it during a call you did not place; use it only after calling back on a saved number. It is one layer and never replaces the callback.
4. ☐ Reduce public voice samples when practical: use the carrier’s default voicemail greeting and limit public posts that contain long, clear family speech. Do not rely on audio quality to identify a clone.



5. ☐ For money, require two-person confirmation through a second channel. No gift cards, cryptocurrency, wire, cash courier, or payment-app transfer because of an inbound urgent request.
6. ☐ For bank, police, court, tax, hospital, or company claims, find the official number yourself and call it. Caller ID can be spoofed.
7. ☐ Practice once. A two-minute family drill is more useful than hoping everyone remembers under stress.

Suggested family script: “We never send money or codes from an incoming call or message. We hang up, call back on a saved number, and use our private phrase. No one gets in trouble for slowing down—and no one gets in trouble for telling us they clicked something, either.”

MODULE COMPLETE ☐ Date: _____

14. Safe use of ChatGPT and AI agents

THE SAFE BOUNDARY AI may research, summarize, draft, compare, and prepare. A person should verify and execute high-impact actions involving money, identity, legal rights, medical care, security settings, or public communications.

1. ☐ Do not paste passwords, one-time codes, security-key prompts, recovery keys, Social Security numbers, full card/bank numbers, private keys, seed phrases, or unredacted identity documents into a chat.
2. ☐ ChatGPT mobile: open the sidebar → tap your profile → Data Controls → turn off Improve the model for everyone if you do not want new chats used to improve models. Settings may change by plan and version.
3. ☐ Use Temporary Chat for a conversation you do not want in history or memory. It is not a vault: OpenAI says a copy may be retained for up to 30 days for safety, and data sent to third-party actions follows their policies.
4. ☐ Treat every connector as a new trust boundary: it lets the AI read information after email or message encryption has already delivered it. Default to no connector for email, Messages, password managers, banking, brokerage, tax, or recovery-code data. If a connector is necessary, use the narrowest scope and disconnect it afterward.
5. ☐ Give narrow instructions: “Draft a reply; do not send it” or “List three options; do not purchase.” Avoid “handle everything in my email.”
6. ☐ If an agent needs a login, enter credentials only in the product’s secure takeover/login flow—not in the chat. Do not allow an agent to read password-reset emails or one-time codes unless absolutely necessary.
7. ☐ Before approving an action, independently check the destination, recipient, attachments, amount, account, and whether private data will be shared. Stop if anything is unexpected.



14. Safe use of ChatGPT and AI agents, continued

⚠ ADVANCED — ASK FOR HELP IF UNSURE ChatGPT Lockdown Mode limits web and connected-app capabilities and may reduce convenience.

8. ☐ For sensitive work, use logged-out access where possible. Optional: ChatGPT → Settings → Security → Advanced security → Lockdown Mode, if available and if you accept reduced capabilities.
9. ☐ Assume websites, emails, files, and documents may contain prompt injection—malicious instructions meant to mislead an agent, such as a webpage telling it to email your codes or upload a private file. Safeguards reduce risk but do not eliminate it.

MODULE COMPLETE ☐ Date: _____

Optional advanced protections: who should consider them

Consider these if you are a public figure, journalist, activist, executive, administrator, cryptocurrency holder, custodian of valuable family assets, or someone facing stalking or targeted harassment.

⚠ ADVANCED — ASK FOR HELP IF UNSURE These settings can reduce convenience or make account recovery harder. Use them only with a tested recovery plan.

- Two physical FIDO security keys (small physical sign-in devices) on Apple, primary email, password manager, and other critical accounts.
- Apple Lockdown Mode: Settings → Privacy & Security → Lockdown Mode. This limits features and is not needed for most people.
- Advanced Data Protection for iCloud, after recovery contacts/keys are tested and documented.
- A dedicated device or separate browser profile for financial activity, with minimal apps and extensions.
- ChatGPT Lockdown Mode: Settings → Security → Advanced security. Limit connected apps and never give an agent access to financial, password-manager, or recovery-code data.



If something feels wrong

THINK YOU MADE A MISTAKE? TELL SOMEONE IMMEDIATELY. Do not be embarrassed and do not try to fix it alone. Minutes can matter.

No one gets in trouble for telling the family they clicked, paid, shared, or installed something.

USE THE CARD FIRST STOP → HANG UP → CALL BACK → VERIFY → THEN ACT. The Emergency Card is the 30-second summary; this page is the follow-through runbook.

1. ☐ Stop responding. Do not click, pay, install software, share anything, or let anyone control your screen. Tell a trusted person now.
2. ☐ Sent money by bank, wire, or app: Call the bank, wire service, or payment-app fraud team immediately; ask whether the transfer can be stopped or reversed.
3. ☐ Gave a password: If the exposed password was used for primary email (or reused there), secure email first; otherwise secure the affected account. Review devices, passkeys, recovery, and forwarding.
4. ☐ Code / sign-in approved: Call the affected institution immediately. Review sign-ins, devices, recovery methods, and enrolled passkeys.
5. ☐ Installed remote access: Disconnect the device from the internet and get trusted help.
6. ☐ Lost or stolen iPhone: Mark as Lost from another device at [iCloud.com/find](https://icloud.com/find). If stolen, do not add a callback number; if merely lost, a contact number may help. Never remove the device from Find My—even after remote erase—because that removes Activation Lock. Ignore inbound ‘we found it’ or Apple Support contacts; never share the passcode, Apple Account password, or a code.
7. ☐ Cellular lost / eSIM changed: From another phone, call carrier fraud and request an immediate line lock; this may be SIM, eSIM, or port-out fraud.
8. ☐ Gave SSN or identity details: Freeze credit; follow the recovery plan at IdentityTheft.gov.
9. ☐ Unsure what happened: Stop communicating and call a trusted family member.

CALLBACK RULE Use a saved number, official app, card, statement, or official site—never the incoming number, link, caller ID, or search ad. Use the family challenge or phrase only after you place the callback.

Record times, names, case numbers, screenshots, receipts, and transaction details. Report fraud at ReportFraud.ftc.gov; for internet-enabled financial crime, also file at IC3.gov. Contact local law enforcement when appropriate.



Sources and verification notes

Front-to-back source audit completed August 28, 2026. The guide was checked in reading order against the official Apple, CISA, FTC, IRS, USPS, LinkedIn, Google, OpenAI, Innovis, and ChexSystems sources below. Provider-specific menus and protections vary; use the provider's current help page when a label differs. This guide is educational, not individualized legal, financial, or cybersecurity advice. Maintained by Banis Risk & Resilience • BanisRisk.com • Verified against iOS 26.x and provider guidance available August 28, 2026. CHANGELOG v2026.08.2: added Banis Risk & Resilience identity, maintainer, website, and standardized source packaging. The safety protocol is unchanged from v2026.08.1.

PAGES 2-3 - IPHONE, PERMISSIONS, APPLE ACCOUNT

- [Apple: Security releases](https://support.apple.com/100100)
- [Apple: iOS 26.3 security content](https://support.apple.com/en-us/126346)
- [Apple: iOS 26 enterprise notes \(automatic SDP enablement\)](https://support.apple.com/en-ie/125073)
- [Apple: Stolen Device Protection](https://support.apple.com/120340)
- [Apple: Locked apps with Stolen Device Protection](https://support.apple.com/en-us/125690)
- [Apple: If an iPhone was stolen](https://support.apple.com/120837)
- [Apple: Control what you share on iPhone](https://support.apple.com/guide/iphone/control-what-you-share-iph6e7d349d1/26/ios/26)
- [Apple: Safety Check](https://support.apple.com/guide/personal-safety/safety-check-iphone-ios-16-ips2aad835e1/web)
- [Apple: Apple Account security](https://support.apple.com/102614)
- [Apple: Recovery contacts](https://support.apple.com/102641)
- [Apple: Security keys for Apple Account](https://support.apple.com/guide/iphone/use-security-keys-iph5acc5b28c/26/ios/26)
- [Apple: Advanced Data Protection](https://support.apple.com/guide/iphone/use-advanced-data-protection-iph584ea27f5/26/ios/26)
- [Apple: Passkeys on iPhone](https://support.apple.com/guide/iphone/use-passkeys-iphf538ea8d0/26/ios/26)

PAGES 3-6 - EMAIL, PASSWORDS, MONEY, CELLULAR, BROWSERS

- [FTC: Recover a hacked email or social account](https://consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account)
- [CISA: Mobile guidance \(high-risk guidance adapted for household use\)](https://www.cisa.gov/resources-tools/resources/mobile-communications-best-practice-guidance)
- [CISA: Phishing-resistant MFA](https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf)
- [Google: Secure a hacked account](https://support.google.com/accounts/answer/6294825)
- [Apple: Safari privacy controls](https://support.apple.com/guide/iphone/browse-the-web-privately-iphb01fc3c85/26/ios/26)
- [Apple: iCloud Private Relay](https://support.apple.com/102602)

PAGES 6-9 - EVERYDAY SAFETY, ROUTER, IDENTITY, BACKUPS, VOICE

- [FTC: Social-media ads and scams](https://consumer.ftc.gov/consumer-alerts/2026/08/are-ads-social-media-vetted-or-checked-scams-heres-what-know)
- [FTC: Top scams that start on social media](https://consumer.ftc.gov/consumer-alerts/2026/04/how-spot-top-scams-started-social-media)
- [FTC: QR-code scams](https://consumer.ftc.gov/consumer-alerts/2023/12/scammers-hide-harmful-links-qr-codes-steal-your-information)
- [LinkedIn: Search for jobs safely](https://www.linkedin.com/help/linkedin/answer/a9535030)

- [FTC: Secure a home Wi-Fi network](https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network)
- [FTC: Credit freezes and fraud alerts](https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts)
- [FTC: Protect a child from identity theft](https://consumer.ftc.gov/articles/how-protect-your-child-identity-theft)
- [Innovis: Security freeze](https://www.innovis.com/personal/securityFreeze)
- [ChexSystems: Place a security freeze](https://www.chexsystems.com/security-freeze/place-freeze)
- [IRS: Get an Identity Protection PIN](https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin)
- [IRS: IP PIN frequently asked questions](https://www.irs.gov/identity-theft-fraud-scams/frequently-asked-questions-about-the-identity-protection-personal-identification-number-ip-pin)
- [USPS: Informed Delivery](https://informedelivery.usps.com/)
- [FTC: Prescreened credit offers](https://consumer.ftc.gov/articles/what-know-about-prescreened-offers-credit-and-insurance)
- [Apple: Back up iPhone with iCloud](https://support.apple.com/108366)
- [CISA: Ransomware backup and restore guidance](https://www.cisa.gov/stopransomware/ransomware-guide)
- [FTC: Family emergency and voice-clone scams](https://consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money)

PAGES 9-11 - AI AGENTS AND INCIDENT RESPONSE

- [OpenAI: ChatGPT agent safety and privacy](https://help.openai.com/en/articles/11752874-chatgpt-agent)
- [OpenAI: Data Controls](https://help.openai.com/en/articles/7730893-datacontrols-faq)
- [OpenAI: Temporary Chat](https://help.openai.com/en/articles/8914046-temporary-chat-faq)
- [OpenAI: Understanding prompt injection](https://openai.com/safety/prompt-injections/)
- [OpenAI: ChatGPT parental controls](https://help.openai.com/en/articles/12315553-parental-controls-in-chatgpt)
- [OpenAI: Lockdown Mode](https://help.openai.com/en/articles/20001061)
- [FTC: Verification codes](https://consumer.ftc.gov/consumer-alerts/2024/03/whats-verification-code-why-would-someone-ask-me-it)
- [FTC: Mobile payment apps](https://consumer.ftc.gov/articles/mobile-payment-apps-how-avoid-scam-when-you-use-one)
- [FTC: What to do if you were scammed](https://consumer.ftc.gov/articles/what-do-if-you-were-scammed)
- [FBI IC3: Report internet-enabled crime](https://complaint.ic3.gov/)