

WHY NOW

BANIS RISK & RESILIENCE
COMMUNITY CYBER RESILIENCE

The rules of online safety have changed.

AI can make a fake bank representative sound professional, a cloned relative sound real, and fraudulent websites and messages look authentic.

YOU NO LONGER NEED TO RECOGNIZE THE FAKE.**Build protections that prevent it from succeeding. Start with these five actions today.**

KIT MAP Fridge = Emergency Card • Do today = this plan • Exact settings = Complete Guide

1

Update every device

3 MIN PER DEVICE



Open Software Update and install the current point release today—even if Automatic Updates is on. Then confirm automatic updates are enabled.

iPhone: Settings → General → Software Update

2

Confirm iPhone theft protections

5 MIN



On iOS 26.4+, Apple turns on Stolen Device Protection for new setups and restores, and when a device running 26.4 updates later; still confirm it is on. It requires a passcode, biometrics, Apple two-factor, Find My, and Significant Locations. Consider Security Delay: Always.

Settings → Face ID & Passcode → Stolen Device Protection

3

Protect Apple and primary email

5 MIN



Confirm two-factor authentication is on. Use a passkey when offered. Never approve a sign-in you did not start.

Apple: Settings → [your name] → Sign-In & Security

4

Turn on money alerts

5 MIN



At every bank and brokerage, enable alerts for logins, new devices, transfers, new payees, profile changes, and purchases.

Official app → Profile or Settings → Security / Alerts

5

Create and practice the family rule

10 MIN



Agree on a private challenge or two-part phrase, then rehearse one scam call. Never act on money, codes, secrecy, or remote access during the original contact.

*Use the phrase only after you place the callback—never on an inbound call.***NEVER SHARE** Codes, passkey prompts, or recovery secrets with anyone who contacted you.

HOUSEHOLD OWNER: _____ SETUP PARTNER: _____

THIS WEEK

BANIS RISK & RESILIENCE
COMMUNITY CYBER RESILIENCE

Break the chain

These protections keep one stolen password, phone, or identity detail from becoming a larger loss.

1

Use a password manager and passkeys

15 MIN PER ADULT



Save unique passwords instead of reusing them. Fix email, Apple, financial, carrier, and social accounts first. Accept “Create a passkey” when offered.

iPhone: Passwords app • AutoFill: Settings → General → AutoFill & Passwords

2

Protect your phone number

10 MIN PER LINE



Add a carrier PIN and port-out or number lock. Ask how eSIM transfers are approved. After stronger recovery is tested, remove SMS as a sign-in or recovery fallback where permitted.

Call the number shown on the carrier's official bill or website.

3

Protect every identity in the home

START TODAY



Freeze adult credit at all three bureaus. For children under 16, a parent or guardian requests the freezes; ages 16–17 may request or remove their own. A freeze does not lock existing cards. Request an IRS IP PIN for each eligible taxpayer and dependent; under 18, use Form 15227 or a Taxpayer Assistance Center.

Official starts: IRS.gov/IPPIN • Equifax • Experian • TransUnion

4

Secure the home router

10 MIN



Install router updates. Use WPA3 or WPA2-AES, a unique Wi-Fi password, and a different administrator password. Disable remote administration if unused.

Use the router maker's official app or support page.

5

Confirm backups

5 MIN



Turn on iCloud Backup and verify a recent successful backup. Keep a separate backup of irreplaceable computer files and photos.

iPhone: Settings → [your name] → iCloud → iCloud Backup

WEEK COMPLETE ☐

Completed: _____ Reviewed with: _____

AI BOUNDARY

Keep secrets out. Give narrow tasks. Review every recipient, amount, attachment, and final action.

EVERYDAY HABITS

BANIS RISK & RESILIENCE
COMMUNITY CYBER RESILIENCE

Shop, scroll, and connect safely

AI can fabricate convincing ads, stores, reviews, profiles, recruiters, voices, and customer support.

THE ONE RULE TO REMEMBER**SEE IT IN A FEED → LEAVE THE FEED → OPEN THE OFFICIAL APP → VERIFY**

1

An ad or QR code is not an endorsement

Do not buy through an ad or use an unexpected QR code for login or payment. Open the official app, bookmark, or known address.

2

Verify unfamiliar sellers

Search the name plus “scam,” “complaint,” and “reviews.” Check independent sources, return terms, seller history, and unrealistic prices.

3

Use safer payment

Prefer a credit card or protected checkout. Avoid wires, cryptocurrency, gift cards, debit cards, checks, and unprotected transfers.

4

Slow trust is still unproven

Weeks of chat, photos, or video do not prove identity. A new relationship moving toward investing, crypto, recovery help, or secrecy is a stop.

5

Share less on social media

Limit who can see your birthday, relatives, location, travel, school, workplace, contacts, and routines.

6

Verify jobs and professional contacts

Confirm jobs on the employer's official careers page. Never pay for equipment or provide banking, SSN, or identity documents before secure onboarding.

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.

WHEN SOMETHING FEELS WRONG

BANIS RISK & RESILIENCE
COMMUNITY CYBER RESILIENCE

Stop. Verify. Then act.

A real family member, bank, employer, or support team can tolerate independent verification.

THINK YOU MADE A MISTAKE? TELL SOMEONE IMMEDIATELY.

Do not be embarrassed and do not try to fix it alone. Minutes can matter.

STOP → HANG UP → CALL BACK → VERIFY → THEN ACT

WHAT JUST HAPPENED?

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.
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.
Code / sign-in approved	Call the affected institution immediately. Review sign-ins, devices, recovery methods, and enrolled passkeys.
Installed remote access	Disconnect the device from the internet and get trusted help.
Lost or stolen iPhone	DO: From another device, go to iCloud.com/find and Mark as Lost. If stolen, leave the contact field blank. Never remove it from Find My. DO NOT: Answer 'we found it' or Apple Support contacts, or share the passcode, Apple Account password, or a code.
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.
Gave SSN or identity details	Freeze credit; follow the recovery plan at IdentityTheft.gov.
Unsure what happened	Stop communicating and call a trusted family member.

FAMILY 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.

SAVE THESE OFFICIAL ADDRESSES

Lost iPhone: iCloud.com/find • Identity recovery: IdentityTheft.gov

Fraud reports: ReportFraud.ftc.gov / IC3.gov • Financial loss: call the provider immediately

AI SAFETY: Keep secrets out • Give narrow tasks • Verify every recipient, amount, attachment, and final action

Menus vary by device, provider, and app version.

SOURCE AUDIT

BANIS RISK & RESILIENCE
COMMUNITY CYBER RESILIENCE

Official sources

Primary and provider sources checked August 28, 2026. Titles and printed URLs lead to the source.

TODAY — UPDATES, IPHONE, ACCOUNTS, CALLBACK

- [Apple: Security releases](https://support.apple.com/100100)
support.apple.com/100100
- [Apple: Stolen Device Protection](https://support.apple.com/120340)
support.apple.com/120340
- [Apple: Locked apps with Stolen Device Protection](https://support.apple.com/en-us/125690)
support.apple.com/en-us/125690
- [Apple: Apple Account security](https://support.apple.com/102614)
support.apple.com/102614
- [Apple: Recovery contacts](https://support.apple.com/102641)
support.apple.com/102641
- [FTC: Recover a hacked email or social account](https://consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account)
consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account
- [FTC: Family emergency and voice-clone scams](https://consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money)
consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money

THIS WEEK — PASSWORDS, PHONE, IDENTITY, ROUTER, BACKUP

- [CISA: Mobile guidance \(high-risk guidance adapted for household carrier/SIM steps\)](https://www.cisa.gov/resources-tools/resources/mobile-communications-best-practice-guidance)
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)
www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- [FTC: Credit freezes and fraud alerts](https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts)
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)
consumer.ftc.gov/articles/how-protect-your-child-identity-theft
- [IRS: Get an Identity Protection PIN](https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin)
www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin
- [FTC: Secure a home Wi-Fi network](https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network)
consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network
- [Apple: Back up iPhone with iCloud](https://support.apple.com/108366)
support.apple.com/108366

EVERYDAY AND EMERGENCY

- [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)
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)
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)
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)
www.linkedin.com/help/linkedin/answer/a9535030
- [Apple: If an iPhone was stolen](https://support.apple.com/120837)
support.apple.com/120837
- [FTC: What to do if you were scammed](https://consumer.ftc.gov/articles/what-do-if-you-were-scammed)
consumer.ftc.gov/articles/what-do-if-you-were-scammed
- [FBI IC3: Report internet-enabled financial crime](https://complaint.ic3.gov)
complaint.ic3.gov
- [OpenAI: ChatGPT agent safety and privacy](https://help.openai.com/en/articles/11752874-chatgpt-agent)
help.openai.com/en/articles/11752874-chatgpt-agent

AUDIT / PRINT NOTE

The plan uses stable family rules and qualifies settings that vary by bank, carrier, browser, device, country, or app. Recheck provider-specific menus before the February 2027 review date. Print pages 1–4; keep page 5 digital for live links.