

KEEP NEAR THE PHONE

BANIS RISK & RESILIENCE
COMMUNITY CYBER RESILIENCE

Family Cyber Emergency Card

Use this the moment a call, message, payment, account, phone, or device 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.

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.

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.

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.

FILL THESE IN BEFORE AN EMERGENCY — WRITE THE LOCATION, NOT THE SECRET

Bank/payment-app fraud: _____ Brokerage/wire fraud: _____
 Carrier fraud: _____ Police / case notes: _____
 Trusted callback #1: _____ Trusted callback #2: _____
 Apple recovery contact: _____ Phrase is stored: _____
 iCloud.com/find • IdentityTheft.gov • ReportFraud.ftc.gov • IC3.gov • Text scams: 7726

SOURCE AUDIT

BANIS RISK & RESILIENCE
COMMUNITY CYBER RESILIENCE

Emergency Card sources

Official guidance checked Aug. 28, 2026. Links are clickable in the PDF.

PRINTING NOTE Print page 1 on 80–100 lb cardstock; lamination and a phone-table hook are optional.

Lost or stolen iPhone — Mark as Lost, Find My, and fake Apple contacts

support.apple.com/120837

Sent money by bank, wire, or payment app — contact the provider immediately

consumer.ftc.gov/articles/what-do-if-you-were-scammed

Password exposure — recover the account, review devices, recovery, and forwarding

consumer.ftc.gov/articles/how-recover-your-hacked-email-or-social-media-account

Verification codes — use them only for a sign-in you started

consumer.ftc.gov/consumer-alerts/2024/03/whats-verification-code-why-would-someone-ask-me-it

Remote-access and fake technical-support contacts

consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

Family-emergency and voice-clone scams — call the person back yourself

consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money

Carrier/SIM protections — adapted from CISA guidance written for highly targeted people

www.cisa.gov/resources-tools/resources/mobile-communications-best-practice-guidance

Identity recovery and credit freezes

consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

Report internet-enabled financial crime to the FBI Internet Crime Complaint Center

complaint.ic3.gov

Forward unwanted scam texts to 7726 (SPAM)

consumer.ftc.gov/consumer-alerts/2026/05/how-are-scammers-trying-reach-you

Audit method: each source above maps to a specific action on page 1. CISA mobile guidance is identified as high-risk guidance adapted for household use. Product instructions can still change.