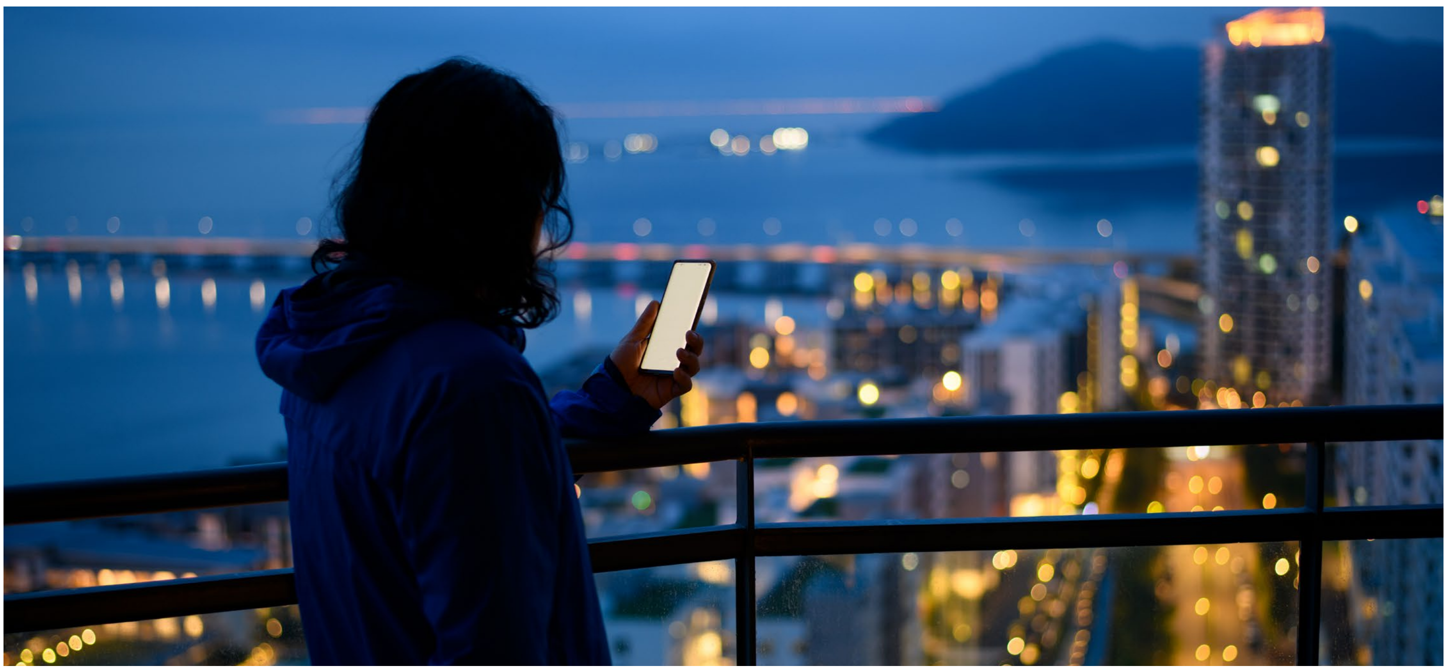
MARINER

The family fraud drill:

Guardrails for texts, money moves and impersonation scams

Most families already have safety habits they follow without thinking twice: Lock the doors, buckle the seat belt, check in when travel plans change.



Fraud prevention can work the same way. A few simple household rules can help everyone slow down, verify what is real and make more deliberate decisions when an unexpected text, call or money request shows up.

That matters because impersonation scams remain one of the most common forms of fraud. According to the Federal Trade Commission, imposter scams were the most-reported fraud category in 2025, with people reporting $3.5 billion in losses.[1]

The good news: Your family doesn't need a complicated cybersecurity plan to reduce risk. A shared fraud drill can give everyone a simple process to follow before a scammer creates urgency.

How can your family use this checklist?

A family fraud drill is a short checklist your household agrees to follow when something feels suspicious. Review it together, choose the items that matter most and revisit the plan a few times a year.

The goal is simple: Pause, verify and involve the right person before acting.

The family fraud drill checklist

☐ Choose a family code word

Pick a word or short phrase only trusted family members know. Use it for any urgent message involving an emergency, travel issue, medical concern, arrest or request for money.

☐ Pause when a message creates urgency

Slow down anytime a message asks for secrecy, pressures you to act immediately or makes the situation feel like an emergency. A few extra minutes can make it easier to spot something that does not feel right.

☐ Create a call-back rule

If someone claims to be a child, parent, grandchild, bank employee, government official or advisor, end the conversation and call back using a phone number you already know and trust.

☐ Avoid links and phone numbers from unexpected messages

Do not rely on contact information included in a suspicious text, email or voicemail. Use a saved number, an official statement, the back of a card or another verified source.

☐ Require a second review for unexpected money requests

Any unexpected request for a wire transfer, payment app transaction, cryptocurrency purchase, gift card, new bank instructions or urgent account transfer should be reviewed by another trusted person before anyone acts.

☐ Teach kids and teens when to bring in an adult

Ask children and teens to show a parent or trusted adult any message involving money, passwords, verification codes, account access or secrecy. A simple rule can help: If it feels urgent or private, bring in an adult.

☐ Talk with aging parents before a scam occurs

Walk through common scam scenarios calmly and respectfully. Consider account alerts, trusted contacts and a shared rule that large or unusual transactions get a second review.

☐ Keep verification codes private

Never share a one-time passcode, password reset code or multifactor authentication code with someone who contacts you unexpectedly. If someone asks for a code, pause and verify directly.

☐ Verify new payment instructions

Confirm any new or changed payment instructions using a known phone number or in-person conversation. This is especially important for wires, real estate transactions, tuition payments, charitable gifts and large family transfers.

☐ Treat secrecy as a warning sign

Be cautious if someone says not to tell your spouse, child, parent, advisor, banker or attorney. Scammers often use secrecy to keep another trusted person from spotting the problem.

☐ Strengthen account protections

Use strong, unique passwords and turn on multifactor authentication where available. Set alerts for large withdrawals, new payees, password changes and logins from new devices.

☐ Limit what your family shares publicly

Review what is visible online, including birthdays, school names, travel plans, pet names, family relationships and milestone events. The less personal information available publicly, the less scammers have to work with.

☐ Build a trusted contact list

Keep a short list of verified phone numbers for family members, your bank, credit card companies, advisor, attorney and insurance provider. Store it somewhere easy to access so no one has to rely on search results during a stressful moment.

☐ Know what to do if something happens

Stop communicating with the sender or caller. Contact the financial institution involved, change relevant passwords, review account activity and alert your advisor, bank or credit card company as appropriate.

☐ Revisit the plan

Review the code word, trusted contacts and money-move rules twice a year. A quick family check-in can keep the process familiar without making it feel overwhelming.

What can you say when something feels off?

You don't need to explain, argue or keep the conversation going. A simple response is enough.

For an unexpected money request:

"I don't make financial decisions from unexpected calls or messages. I'm going to verify this directly."

For a family emergency message:

"I need the family code word before we go any further."

For a bank or account alert:

"I'll call the institution directly using the number I already have."

The bottom line

Scammers often depend on pressure, urgency and confusion. Families can respond with something stronger: a calm, simple system. When everyone knows what to do, it becomes easier to pause, verify and make decisions with a clearer head.

You may also want to talk with your advisor about how this checklist fits into your broader family financial conversations, especially around trusted contacts, account alerts and large transactions.

For more information visit: **mariner.com**

[1]Federal Trade Commission, FTC Data Show People Reported Losing $3.5 Billion to Imposter Scams in 2025.