

Before you click, call, or pay

Your family scam safety checklist. Keep this page by your phone. Use the online guide when you want more detail.

1 Give yourself a pause

An unexpected money request does not need an immediate answer. End the conversation before deciding what to do.

2 Check through a trusted route

Call the person or company yourself, using a number you already trust. Do not use the number, link, or QR code in the suspicious message.

3 Talk it through

Choose someone you can call before sending money or sharing information. Scammers may try to keep you from asking for help.

“I’m going to hang up and check this through a number I already trust.”

My trusted contact: _____

Phone: _____

Choose a private family code phrase together. Keep it off this sheet and off social media. It is an extra check, not a substitute for calling back.

When a call or text feels urgent

A call from your bank

A caller says your money is at risk and tells you to move it to a safe account. Hang up. Call the number on your bank card or use the official app. Do not share a verification code or transfer money at an unexpected caller's direction.

Say: "I'll call my bank using the number on my card."

A supposed family emergency

A familiar voice is not enough to prove who is calling. Call your relative on their usual number. If you cannot reach them, check with another trusted family member before sending money.

Say: "I'm going to call you back and check with the family."

A toll, ticket, or delivery text

A small amount can still be a trap. Do not use its payment link or QR code. Check through the real agency's website or app. Use your phone's report-junk option, or forward an unwanted text to 7726, then delete it.

Remember: Caller ID, a logo, or a convincing voice is not independent verification.

When an offer asks for access or money

An unexpected bill or warning

Do not call a number in an alarming computer warning or unexpected bill. Open the company's official app or website yourself. Do not give an unexpected caller remote access to your computer.

For airline help: Use the airline's official app or your booking confirmation. Search results can include impostors.

An online friend offers investing help

A relationship can be used to introduce a fake investment. A professional-looking website or early withdrawal does not establish that it is legitimate. Get an independent second opinion. Do not pay more money to unlock supposed profits on a suspicious platform.

Say: "I don't send money or make investments through people I've met online."

A job asks you to deposit money

Stop if you must pay to unlock earnings or complete another level of tasks. Check the job through the real employer. A small early payment does not prove the offer is genuine.

Say: "I won't deposit money to receive pay."

If you already clicked or paid

Money sent

Contact your bank, card issuer, or payment service immediately. Ask whether the transaction can be stopped or reversed. Recovery is not guaranteed.

Password or device access shared

Change affected and reused passwords from a trusted device. If you allowed remote access, disconnect the affected device and contact a trusted support provider.

Identity information shared

Go directly to IdentityTheft.gov for a recovery plan. Save messages, receipts, and dates. Keep private details out of public comments.

Report and get help

Use ReportFraud.ftc.gov. Internet crime can also be reported at IC3.gov. Do not pay someone upfront to recover lost money. If someone is in immediate danger, call 911.

Read the full guide and its sources

tesh-scam-safety.johntesh5.workers.dev

Based on radio topics supplied by John Tesh, with guidance checked against the FTC, FBI, and SEC. Reviewed September 29, 2026. This educational guide cannot verify a particular caller, message, or investment.