WTM MEDIA
Why These Matter

AI & EVERYDAY SAFETY / VISUAL INTELLIGENCE

# When a Familiar Voice Asks for Money

You do not need to detect a fake voice. You need a way to verify the request.

Inside: a callback route, a family plan and a calm response if money has already gone.



Editorial illustration: a couple checking an independent contact route.

WTM MEDIA
Why These Matter

# Leave the incoming channel. Verify independently.

A familiar voice, realistic video or known account is not enough to approve an urgent payment.

01

## End the contact

Do not use a link or number supplied in the request.

02

## Call a known number

Use a contact you already trust, not caller ID.

03

## Try a trusted backup

Reach another relative or contact through a separate route.

04

## Check before paying

Confirm the situation and destination. Unverified? Do not send.

If someone may be in immediate danger, independently contact the appropriate local emergency service. An emergency claim is not proof that a payment request is genuine.

FTC emergency-scam advice

WTM MEDIA
Why These Matter

# Agree on a route everyone can use

Keep the details private and accessible to the people who need them.

| | |
|---|---|
| Primary contact | A known phone number already saved. |
| Backup contact | Someone who can independently reach the person. |
| Extra check | A private family phrase, not a public fact or account password. |
| Accessibility | A route that works with hearing, language and device needs. |

FBI / IC3 guidance, 15 May 2025



Editorial illustration: three adults discussing a family contact plan.

A family phrase is an extra check, not sole proof. It can be disclosed, guessed or overheard. Keep independent contact as the foundation.

# Four habits that reduce avoidable exposure

Good account security helps. It cannot guarantee that every message or call is genuine.



Editorial illustration: two people reviewing account settings.

## Use strong, distinct passwords

A reputable password manager can help you maintain them.

## Turn on two-factor authentication

Never give a caller your one-time authentication code.

## Treat unexpected links cautiously

Open the service through its known app or website.

## Share the plan without blame

Make it easy to ask for help and to stop a pressured payment.

FTC: protect your personal information

FBI / IC3: impersonation and authentication codes

WTM MEDIA
Why These Matter

# Act promptly. Keep the facts. Avoid blame.

Recovery is not guaranteed, but quick contact may improve the chance of limiting further harm.

01 **Contact the payment provider**

Use its official app or number. Explain exactly what happened and ask whether the payment can be stopped or recovered.

02 **Preserve the evidence**

Keep messages, receipts, payment details and a timeline. Describe accurately whether you authorised the payment.

03 **Report through an official route**

In the US, FTC and IC3 accept reports. Elsewhere, use the relevant local fraud-reporting and law-enforcement channels.

04 **Reject recovery-fee promises**

A new caller who guarantees to recover the money may be running another scam. Keep a trusted person involved.

FTC: what to do if you were scammed

FTC: refund and recovery scams

WTM MEDIA
Why These Matter

# Protect trust by making verification ordinary

A pause is not an accusation. It is a shared family habit.

## Agree today that an urgent request for money triggers a callback. The rule works best when everyone expects it, including the person asking for help.

FTC: fake emergencies

FBI / IC3: impersonation guidance, 15 May 2025

FTC: account and personal-information protection

FTC: response after a scam

FTC: refund and recovery scams

Sources reviewed 8 November 2026. US reporting guidance is not universal.



Editorial illustration: a family sharing an unhurried meal.

No voice test or verification phrase is foolproof. These steps reduce reliance on the incoming channel; they do not guarantee prevention or recovery.