

# Our family verification plan

A familiar voice, photo or video is not proof of identity. Agree on this plan before anyone receives an urgent request for money or information.

## 1. Pause

Do not send money, share a password or verification code, or click a link under pressure.

## 2. End the call and check

Call the person back using a number you already trust. Do not use a number or link supplied in the suspicious message.

## 3. Get a second opinion

If you cannot reach them, contact another trusted person. A family code phrase can help, but it does not replace an independent callback.

## 4. If money or information was sent

Contact your bank or payment provider immediately through its official app or a known number. Report the incident to the appropriate fraud authority or police.

Trusted person + phone number:

---

Backup person + phone number:

---

Agree on any private code phrase offline. Do not write passwords, account details or verification codes on this sheet.

---

Based on FTC independent-callback guidance ([consumer.ftc.gov](https://consumer.ftc.gov)) and FBI guidance ([ic3.gov/psa/2024/psa241203](https://ic3.gov/psa/2024/psa241203)).