# Two-Channel Verification Matrix

If a request arrives on one channel, confirm it on a different one that **you** start, using contact details you already had.

| The request arrives by… | Do NOT use | Safer second channel (you start it) | Tips |
|---|---|---|---|
| **Text message / chat app (SMS, WhatsApp, iMessage)** | Replying to the message; links, buttons, QR codes in it; the number it came from | Call the person or company on a number saved in your contacts, on the back of your card, or in the official app | Real contacts can be reached on the second channel too. If they can't be, that is information. |
| **Incoming phone call** | Caller ID (it can be faked); "press 1"; a number they give you; staying on the line | Hang up, wait, and call back using the number on your card, statement, bill or official website. Use another phone if you can. | Scammers can keep a landline open. Listen for a dial tone before you call back. |
| **Voicemail or voice message** | Calling the number left in the message | Look up the organization's number yourself, or call the family member on their saved number | A voice can be cloned. Ask for the safe word on the callback. |
| **Email** | Links, attachments, "reply" address, phone number in the email | Open the company's app or type its address yourself; or phone using a number from a past statement | Check the sender's actual address, not just the display name. |
| **Social media message / friend request** | Replying; clicking links; moving to a private chat app | Phone or video the person using a number you already had; ask the safe word | A hacked account can send messages that look genuine. |
| **Video call** | Trusting the face or voice alone | Hang up and call back on a saved number; ask the safe word or a question only they can answer | Video can be faked or replayed. |
| **Letter, flyer or QR code in public** | Scanning the QR code; calling the number printed on it | Search for the organization yourself or use its official app; ask a person you trust | Stickers can be placed over genuine QR codes (parking, menus, notices). |
| **At the door or a courier pick-up** | Handing over cash, cards, PINs or devices | Close the door; phone the organization on its official number; contact family | Real agencies do not send couriers to collect money. |
| **Pop-up or browser alert ("virus", "support")** | The number or button in the alert; allowing remote access | Close the browser; restart the device; contact support through the company's official site or app | No genuine alert asks you to phone a number. |

**The rule:** A second channel counts only if you start it with contact information you already trusted **before** this request arrived.


© 2026 Cogitent Press. All rights reserved. Educational use only; not legal or financial advice.